134/2009 Z.z.

VYHLÁŠKA

Národného bezpečnostného úradu

z 26. marca 2009,

ktorou sa ustanovujú podrobnosti o požiadavkách na bezpečné zariadenia na vyhotovovanie časovej pečiatky a požiadavky na produkty pre elektronický podpis (o produktoch elektronického podpisu)

Národný bezpečnostný úrad (ďalej len "úrad") podľa § 9 ods. 1 písm. d) a § 24 ods. 17 zákona č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení zákona č. 214/2008 Z. z. (ďalej len "zákon") ustanovuje:

§ 1
Predmet vyhlášky

Táto vyhláška upravuje
a) podrobnosti o požiadavkách na bezpečné zariadenia na vyhotovovanie časovej pečiatky,
b) požiadavky na produkty pre elektronický podpis.

§ 2
Podrobnosti o požiadavkách na bezpečné zariadenie na vyhotovovanie časovej pečiatky

Bezpečné zariadenie na vyhotovovanie časovej pečiatky podľa § 2 písm. x) zákona je zariadenie, ktoré spĺňa nasledujúce požiadavky:
a) súkromný kľúč a verejný kľúč vydavateľa časovej pečiatky sú vyhotovované kontrolovaným a riadeným spôsobom,
b) súkromný kľúč vydavateľa časovej pečiatky zostáva utajený a sú odstránené riziká, ktoré môžu spôsobiť narušenie jeho integrity,
c) integrita a autenticita verejného kľúča vydavateľa časovej pečiatky slúžiaceho na overenie podpisu, ako aj každého zo súvisiacich parametrov je zabezpečená počas distribúcie prijímateľom,
d) životnosť certifikátu vydavateľa časovej pečiatky nesmie byť dlhšia ako časový interval, počas ktorého zvolený algoritmus a dĺžka kľúča vyhovujú stanovenému účelu,
e) súkromný kľúč vydavateľa časovej pečiatky nesmie byť použiteľný po uplynutí jeho platnosti,
f) bezpečnosť kryptografického hardvéru slúžiaceho na podpisovanie časovej pečiatky nie je znížená ani narušená počas celej jeho životnosti,
g) inštalácia, aktivácia a vyhotovovanie kópií podpisových kľúčov vydavateľa časovej pečiatky v kryptografickom hardvére prebieha vo fyzicky zabezpečených priestoroch dôveryhodnými oprávnenými osobami,
h) inštaláciu, aktiváciu a vyhotovovanie kópií súkromného kľúča vydavateľa časovej pečiatky v kryptografickom hardvére môžu vykonať najmenej dve oprávnené osoby ich súčasnou činnosťou,

i) kryptografický hardvér slúžiaci na podpisovanie časovej pečiatky pracuje v súlade s technicko-prevádzkovou dokumentáciou a bezpečnostnou politikou a pri poruchách možno identifikovať ich príčinu a spôsobené následky,
j) súkromný kľúč vydavateľa časovej pečiatky uložený na kryptografickom hardvére vydavateľa časovej pečiatky musí byť po odstavení kryptografického hardvéru z prevádzky vymazaný,
k) časová pečiatka je vydaná v súlade s prijatou bezpečnostnou politikou a obsahuje správny čas.

§ 3
Požiadavky na produkty na vyhotovenie zaručeného elektronického podpisu

(1) Produkty na uchovávanie súkromných kľúčov a na vyhotovenie zaručeného elektronického podpisu určené pre podpisovateľa alebo overovateľa zaručeného elektronického podpisu spĺňajú požiadavky zákona, ak
a) pracujú so schválenými podpisovými schémami, algoritmami a parametrami týchto algoritmov,
b) je preukázaná zhoda
1. so štandardom uvedeným v prílohe č. 1 prvom bode,
2. s kryptografickými štandardami infraštruktúry verejného kľúča uvedenými v prílohe č. 1 druhom bode,
3. s požiadavkami uvedenými v osobitnom predpise, [1)]
c) úrad pre ne vydal certifikát podľa § 24 ods. 9 zákona.

(2) Softvérové produkty pre vyhotovovanie a overovanie zaručeného elektronického podpisu spĺňajú požiadavky zákona, ak
a) pracujú so schválenými podpisovými schémami, algoritmami a parametrami týchto algoritmov,
b) je preukázaná zhoda
1. so schváleným formátom zaručeného elektronického podpisu,
2. so štandardom uvedeným v prílohe č. 1 prvom bode,
3. s kryptografickými štandardami infraštruktúry verejného kľúča uvedenými v prílohe č. 1 druhom bode,
4. s požiadavkami uvedenými v osobitnom predpise, [1)]
c) vytvárajú certifikačnú cestu - reťazec certifikátov potrebných na overenie platnosti certifikátu podpisovateľa,
d) spracúvajú zoznam zrušených certifikátov, prípadne spracúvajú odpovede z potvrdenia o existencii a platnosti certifikátu,
e) pridávajú časovú pečiatku, ak aplikácia poskytuje funkcionalitu vyhotovenia zaručeného elektronického podpisu s časovou pečiatkou,
f) podporujú čipové karty alebo iné médiá na uloženie kľúčov a certifikátov,
g) úrad pre ne vydal certifikát podľa § 24 ods. 9 zákona.

(3) Informačné systémy správy certifikátov určené najmä pre poskytovateľov akreditovaných certifikačných služieb spĺňajú požiadavky zákona, ak
a) pracujú so schválenými podpisovými schémami, algoritmami a parametrami týchto algoritmov,
b) spĺňajú tieto funkčné vlastnosti:
1. pracujú s hardvérovým modulom na ochranu kľúča certifikačnej autority, ktorý musí spĺňať požadovanú úroveň ochrany kľúča,
2. je preukázaná zhoda so schválenými formátmi kvalifikovaných certifikátov a certifikátov,
3. je preukázaná zhoda so štandardom uvedeným v prílohe č. 1 prvom bode,
4. umožňujú vytvorenie hierarchickej štruktúry certifikačných autorít,
5. umožňujú rozdelenie na certifikačnú autoritu a registračnú autoritu,
6. umožňujú krížovú certifikáciu,
7. umožňujú realizáciu zoznamu zrušených certifikátov, prípadne realizáciu potvrdzovania existencie a platnosti certifikátu,
8. zabezpečujú prevádzku rýchleho a bezpečného adresára,
9. umožňujú uplatňovanie bezpečnostnej politiky, [2)]
10. umožňujú prácu s administrátorskými nástrojmi na správu infraštruktúry verejných kľúčov,

---

[1)] Rozhodnutie Komisie č. 2003/511/ES zo 14. júla 2003 o zverejnení referenčných čísel pre všeobecne uznané normy na produkty pre elektronické podpisy.
[2)] § 10 vyhlášky 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.

11. je preukázaná ich zhoda s kryptografickými štandardami infraštruktúry verejného kľúča uvedenými v prílohe č. 1 druhom bode,
12. umožňujú podporu čipových kariet alebo iných médií na uloženie kľúčov a certifikátov,
13. je preukázaná zhoda s požiadavkami uvedenými v osobitnom predpise, [1)]
c) informačné systémy poskytovateľov akreditovaných certifikačných služieb podľa § 2 písm. l) tretieho bodu zákona umožňujú okrem funkčných vlastností uvedených v písmene b) aj vytváranie časovej pečiatky,
d) úrad pre ne vydal certifikát podľa § 24 ods. 9 zákona.

(4) Kryptografické moduly hardvérovej ochrany kľúča určené najmä pre poskytovateľov akreditovaných certifikačných služieb spĺňajú požiadavky zákona, ak
a) je zabezpečená ochrana pred neautorizovaným odhalením neverejného obsahu kryptografického modulu vrátane kryptografického kľúča v nešifrovanom tvare a ďalších kritických bezpečnostných parametrov,
b) je zabezpečená ochrana pred neautorizovanou a nedetekovateľnou modifikáciou kryptografického modulu vrátane neautorizovanej modifikácie, substitúcie, vloženia a vymazania kryptografického kľúča a ďalších kritických bezpečnostných parametrov,
c) je indikovaný operačný stav kryptografického modulu,
d) je zabezpečená činnosť kryptografického modulu v súlade s technicko-prevádzkovou dokumentáciou, bezpečnostnou politikou a pri poruche možno identifikovať príčinu a spôsobené následky,
e) sú detekované chyby v operáciách kryptografického modulu a je zabránené poškodeniu citlivých údajov a kritických bezpečnostných parametrov ako dôsledku detekovaných chýb,
f) vyhovuje bezpečnostným požiadavkám podľa FIPS-140-2 Bezpečnostné požiadavky na kryptografické moduly na úrovni 3 na ochranu informácií, ktoré nie sú utajovanými skutočnosťami podľa osobitného predpisu,[3)]
g) existuje špecifikácia kryptografického modulu a špecifikácia kryptografického rozhrania,
h) existuje špecifikácia modelu kryptografického modulu vo forme automatu s konečným počtom stavov,
i) dátové vstupy (porty) pre kritické bezpečnostné parametre sú fyzicky oddelené od ostatných dátových vstupov,
j) existuje detekcia narušenia kryptografického modulu a reakcia na porušenie ochrany a krytu,
k) existuje dôveryhodná komunikačná cesta,
l) vstup a výstup kľúča je v šifrovanej podobe alebo ak je priamy vstup a výstup s procedúrami rozdelenia znalostí kľúča,
m) umožňuje vykonať testovanie funkčnosti, pri zapnutí vykonanie samočinného testovania a má implementované testy podmienok prevádzky,
n) existuje overenie identity operátora a overenie, že identifikovaný operátor je autorizovaný vykonávať špecifickú rolu a príslušnú skupinu činností,
o) úrad pre ne vydal certifikát podľa § 24 ods. 9 zákona.

(5) Požiadavky podľa odseku 1 možno primerane uplatniť aj na produkty na vyhotovovanie elektronického podpisu podľa § 3 zákona.

§ 4
Zrušovacie ustanovenie

Zrušuje sa 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).

[3)] Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

§ 5
Záverečné ustanovenia

(1) Touto vyhláškou sa preberajú právne akty Európskych spoločenstiev a Európskej únie uvedené v prílohe č. 2.

(2) Táto vyhláška bola prijatá v súlade s príslušným právnym aktom Európskych spoločenstiev[4)] pod číslom notifikácie 2008/0530/SK.

§ 6
Účinnosť

Táto vyhláška nadobúda účinnosť dňom vyhlásenia.

František Blanárik v. r.

[4)] 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.

Príloha č. 1
k vyhláške č. 134/2009 Z. z.

ZOZNAM ŠTANDARDOV VZŤAHUJÚCICH SA NA PRODUKTY NA VYHOTOVENIE ZARUČENÉHO ELEKTRONICKÉHO PODPISU

1. Certifikát infraštruktúry verejného kľúča a profil zoznamu zrušených certifikátov. Formát je uvedený v zahraničnej norme.[5)]

2. Kryptografické štandardy infraštruktúry verejného kľúča. Formáty sú uvedené v zahraničnej norme.[6)]

[5)] ITU-T RECOMMENDATION X.509 (08/2005) | ISO/IEC 9594-8 : Information technology - open systems interconnection - the directory: public key and attribute certificate frameworks, IETF RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
[6)] EN 14890-1: Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic Services (Aplikačné rozhranie pre smart karty používané ako bezpečné zariadenia pre vyhotovovanie podpisu - časť 1: Základné služby), EN 14890-2: Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Addidional Services (Aplikačné rozhranie pre smart karty používané ako bezpečné zariadenia pre vyhotovovanie podpisu - časť 2: Doplnkové služby), RSA Štandard PKCS#7, PKCS#10, PKCS#11, PKCS#15.

Príloha č. 2
k vyhláške č. 134/2009 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).