63

VYHLÁŠKA
Národného bezpečnostného úradu

z 10. marca 2014,

ktorou sa mení a dopĺňa 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)

Národný bezpečnostný 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 neskorších predpisov ustanovuje:

Čl. I

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) sa mení a dopĺňa takto:

1. V § 1 písm. b) sa na konci vkladá čiarka a pripájajú sa tieto slová: „elektronickú pečať a časovú pečiatku“.

2. V nadpise § 2 sa slovo „vyhotovovanie“ nahrádza slovom „vyhotovenie“.

3. V § 2 uvádzacej vete sa slovo „vyhotovovanie“ nahrádza slovom „vyhotovenie“ a slová „§ 2 písm. x)“ sa nahrádzajú slovami „§ 2 písm. k)“.

4. V § 2 písmeno e) znie:
„e) súkromný kľúč vydavateľa časovej pečiatky sa po uplynutí jeho platnosti zničí bez možnosti obnovy,[1])“.

Poznámka pod čiarou k odkazu 1 znie:
„[1]) Napríklad § 2 ods. 8 vyhlášky Národného bezpečnostného úradu č. 339/2004 Z. z o bezpečnosti technických prostriedkov.“.

Doterajší odkaz 1 sa označuje ako odkaz 1a.

5. § 2 sa dopĺňa písmenom l), ktoré znie:
„l)kryptografický hardvér slúžiaci na podpisovanie časovej pečiatky primerane spĺňa požiadavky podľa § 3 ods. 4.“

6. V § 3 ods. 1 písm. c), ods. 3 písm. d) a ods. 4 písm. o) sa slová „§ 24 ods. 9“ nahrádzajú slovami „§ 24 ods. 10“.

7. V § 3 ods. 2 písm. b) sa vypúšťa štvrtý bod.

8. V § 3 ods. 2 sa vypúšťa písmeno g).

9. V § 3 ods. 3 písm. c) sa slová „§ 2 písm. l)“ nahrádzajú slovami „§ 2 písm. p)“.

10. Za § 3 sa vkladá § 3a, ktorý vrátane nadpisu znie:

„§ 3a

Požiadavky na produkty na vyhotovenie zaručenej elektronickej pečate

(1) Produkty na uchovávanie súkromných kľúčov a na vyhotovenie zaručenej elektronickej pečate určené pre pôvodcu zaručenej elektronickej pečate 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]) kryptografické moduly hardvérovej ochrany kľúča spĺňajú tieto požiadavky primerane,
c) úrad pre ne vydal certifikát podľa § 24 ods. 10 zákona.

(2) Softvérové produkty pre vyhotovenie a overovanie zaručenej elektronickej pečate spĺňajú požiadavky zákona, ak
a) pracujú so schválenými podpisovými schémami, algoritmami a parametrami týchto algoritmov,
b) spĺňajú tieto funkčné vlastnosti:
   1. pracujú s kryptografickým modulom hardvérovej ochrany kľúča, ktorý spĺňa požadovanú úroveň ochrany kľúča, alebo podporujú čipové karty, alebo podporujú iné médiá na uloženie kľúčov a certifikátov,
   2. je preukázaná zhoda so schváleným formátom zaručenej elektronickej pečate,
   3. je preukázaná zhoda so štandardom uvedeným v prílohe č. 1 prvom bode,
c) vytvárajú certifikačnú cestu – reťazec certifikátov potrebných na overenie platnosti certifikátu pôvodcu pečate,
d) spracúvajú zoznam zrušených certifikátov, spracúvajú odpovede z potvrdenia o existencii a platnosti certifikátu alebo podporujú funkcionalitu modulu úradnej komunikácie použitím zoznamu platných kvalifikovaných systémových certifikátov,
e) pridávajú časovú pečiatku, ak aplikácia poskytuje funkciu vyhotovenia zaručenej elektronickej pečate s časovou pečiatkou.

(3) Požiadavky podľa odsekov 1 a 2 možno primerane uplatniť aj na produkty na vyhotovenie elektronickej pečate podľa § 3a zákona.“.

11. Príloha č. 1 vrátane nadpisu znie:

„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. Formáty sú uvedené v technickej norme.[5])
2. Kryptografické štandardy infraštruktúry verejného kľúča. Formáty sú uvedené v technickej norme.[6])“.

Poznámky pod čiarou k odkazom 5 a 6 znejú:

„[5]) ITU-T RECOMMENDATION X.509 | 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]) STN EN 14890-1 Aplikačné rozhranie pre smart karty používané ako bezpečné zariadenia na vyhotovenie podpisu. Časť 1: Základné služby (36 9724), STN EN 14890-2 Aplikačné rozhranie pre smart karty používané ako bezpečné zariadenia na vyhotovenie podpisu. Časť 2: Dodatočné služby (36 9724), RSA Štandard PKCS#7, PKCS#10, PKCS#11, PKCS#15.“.

Čl. II

Táto vyhláška nadobúda účinnosť 15. marca 2014.

Jozef Magala v. r.