539

VYHLÁŠKA
Národného bezpečnostného úradu

z 9. septembra 2002,

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. 8 zákona č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov (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[1]) 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 určené na uchovávanie súkromných kľúčov a na vyhotovenie zaručeného elektronického podpisu vyhovujú požiadavkám, ak
a) pracujú so schválenými podpisovými schémami, algoritmami a parametrami týchto algoritmov,
b) umožňujú využiť nasledujúce funkcie a vlastnosti
   1. obnovu kľúča,
   2. aktualizáciu kľúča,
   3. zálohovanie kľúča,
   4. rozdelenie kľúča,
   5. hardvérovú ochranu kľúča certifikačnej autority, ktorá musí spĺňať úroveň ochrany kľúča uvedenú v prílohe č. 1,
   6. použitie prídavných modulov a šifrovacích softvérových nástrojov,
   7. kompatibilitu so štandardom uvedeným v prílohe č. 2 bode 1,
   8. kompatibilitu so štandardami manažmentu infraštruktúry verejného kľúča,
   9. vytvorenie hierarchickej štruktúry certifikačných autorít,
   10. rozdelenie na certifikačnú autoritu a registračnú autoritu,
   11. krížovú certifikáciu,
   12. realizáciu zoznamu zrušených certifikátov certifikačných autorít,
   13. vytvorenie časovej pečiatky,

[1]) § 2 písm. x) zákona č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov.

14. atribútovú certifikáciu,
15. bezpečnostnú certifikáciu pre certifikačnú autoritu a registračnú autoritu,
16. hromadnú certifikáciu,
17. realizáciu zoznamu zrušených certifikátov,
18. adresárovú štruktúru,
19. protokol prístupu k adresáru,
20. presadenie bezpečnostnej politiky,
21. prácu s protokolom bezpečnej prevádzky elektronického obchodovania,
22. prácu v prostredí virtuálnych privátnych sietí,
23. prácu s administrátorskými nástrojmi na správu infraštruktúry verejných kľúčov,
24. kompatibilitu s kryptografickými štandardami infraštruktúry verejného kľúča uvedenými v prílohe č. 2 bode 2,
25. podporu čipových kariet alebo iných médií na uloženie kľúčov a certifikátov,

c) úrad pre ne vydal certifikát podľa zákona.

(2) Požiadavky podľa odseku 1 možno primerane uplatniť aj na produkty na vyhotovovanie elektronického podpisu[2]).

§ 4

Účinnosť

Táto vyhláška nadobúda účinnosť 1. októbra 2002.

Ján Mojžiš v. r.

[2]) § 3 zákona č. 215/2002 Z. z.

Príloha č. 1
k vyhláške č. 539/2002 Z. z.

FUNKČNÉ POŽIADAVKY NA KRYPTOGRAFICKÝ MODUL HARDVÉROVEJ OCHRANY KĽÚČA

Kryptografický modul hardvérovej ochrany kľúča spĺňa požiadavky, 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 poruchách 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 schváleným bezpečnostným metódam na ochranu neklasifikovaných informácií podľa FIPS-140-2 Bezpečnostné požiadavky na kryptografické moduly,
g) existuje špecifikácia kryptografického modulu a špecifikácie kryptografického rozhrania,
h) existuje špecifikácia modelu kryptografického modulu vo forme automatu s konečným počtom stavov,
i) dátové porty pre kritické bezpečnostné parametre sú fyzicky oddelené od ostatných dátových portov,
j) existuje overovanie identity operátora,
k) existuje detekcia narušenia kryptografického modulu a reakcia na porušenie ochrany a kryty,
l) je použitý vysokoúrovňový jazyk pre implementáciu kryptografického modulu,
m) v operačnom systéme existuje ochrana prostredníctvom návestí a dôveryhodná komunikačná cesta,
n) vstup a výstup kľúča je v šifrovanej podobe alebo ak je priamy vstup a výstup s procedúrami rozdelenia znalostí kľúča,
o) existuje schopnosť poskytovať vykonanie štatistických testov náhodnosti požiadavky,
p) existuje použitie algoritmov na ochranu neklasifikovaných informácií podľa FIPS-140-2 Bezpečnostné požiadavky na kryptografické moduly,
q) sú splnené požiadavky na elektromagnetické interferencie a elektromagnetickú kompatibilitu minimálne v rozsahu podľa FIPS-140-2 Bezpečnostné požiadavky na kryptografické moduly na úrovni 3,
r) pri zapnutí sa vykoná samočinné testovanie,
s) sú implementované a funkčné testy podmienok prevádzky,
t) existuje overenie identity operátora a overenie, že identifikovaný operátor je autorizovaný vykonávať špecifickú rolu a príslušnú skupinu činností.

Príloha č. 2
k vyhláške č. 539/2002 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.[1])
2. Kryptografické štandardy infraštruktúry verejného kľúča. Formáty sú uvedené v zahraničnej norme.[2])

[1]) RFC 2459: Internet X.509.
[2]) RSA Štandard PKCS#7, PKCS#10, PKCS#11, PKCS#12.