**Návrh**

**Vyhláška**

**Národného bezpečnostného úradu**

**z.........................2008,**

**ktorou sa mení a dopĺňa vyhláška Národného bezpečnostného úradu č. 537/2002 Z. z. o formáte a spôsobe vyhotovenia zaručeného elektronického podpisu, spôsobe zverejňovania verejného kľúča úradu, postupe pri overovaní a podmienkach overovania zaručeného elektronického podpisu, formáte časovej pečiatky a spôsobe jej vyhotovenia, požiadavkách na zdroj časových údajov a požiadavkách na vedenie dokumentácie časových pečiatok (o vyhotovovaní a overovaní elektronického podpisu a časovej pečiatky)**

 Národný bezpečnostný úrad (ďalej len „úrad“) podľa § 4 ods. 4 a 5, § 5 ods. 5, § 9 ods. 2 zákona č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov ustanovuje:

**Čl. I**

 Vyhláška Národného bezpečnostného úradu č. 537/2002 Z. .z. o formáte a spôsobe vyhotovenia zaručeného elektronického podpisu, spôsobe zverejňovania verejného kľúča úradu, postupe pri overovaní a podmienkach overovania zaručeného elektronického podpisu, formáte časovej pečiatky a spôsobe jej vyhotovenia, požiadavkách na zdroj časových údajov a požiadavkách na vedenie dokumentácie časových pečiatok (o vyhotovovaní a overovaní elektronického podpisu a časovej pečiatky) sa mení a dopĺňa takto:

1. § 1 sa dopĺňa písmenom g), ktoré znie:

 „g) formát, obsahové náležitosti a spôsob zverejňovania podpisovej politiky.“.

1. V § 2 písm. g) sa slovo „údaj“ nahrádza slovami „objektový identifikátor“ a na konci sa pripájajú tieto slová „ktorý prideľuje úrad,“.
2. § 2 sa dopĺňa písmenom k), ktoré znie:

 „k) vydavateľom podpisovej politiky subjekt, ktorý prostredníctvom podpisovej

 politiky definuje špecifické, technické a   procedurálne pravidlá pre vytvorenie

 a overenie zaručeného elektronického podpisu.“.

1. V § 3 ods. 4 sa vypúšťa slovo „kvalifikovaných“ trikrát.
2. V § 4 odsek 4 znie:

 „(4) Formát, obsahové náležitosti a štruktúra podpisovej politiky sú uvedené

 v prílohe č. 2.“.

6. Za § 4 sa vkladá § 4a, ktorý vrátane nadpisu znie:

„§ 4a

Spôsob zverejňovania podpisovej politiky

 (1) Vydavateľ podpisovej politiky ju predkladá na schválenie úradu.

 (2) Súlad podpisovej politiky podľa odseku 1 s   formátom, obsahovými

 náležitosťami a štruktúrou podľa prílohy č.1 overuje úrad.

 (3) Ak podpisová politika spĺňa požiadavky podľa odseku 2, zverejňuje ju úrad na

 svojej internetovej stránke a zaraďuje do zoznamu schválených podpisových politík.

 (4) Zoznam zverejňuje úrad vo forme podpísaného textového dokumentu,

 obsahujúceho názov súboru, digitálny odtlačok, dátum platnosti, identifikátor a oblasť

 použitia podpisovej politiky.“.

7. V § 6 sa slová „v prílohe“ nahrádzajú slovami „v prílohe č. 1“.

8. V § 7 ods. 3 a 4 sa slovo „ustanovenému“ nahrádza slovom „ustanoveného“.

9. V § 7 ods. 5 písmeno b) znie:

 „b) elektronický podpis časovej pečiatky vydavateľa je platný; pre stanovenie jeho

 platnosti sa ustanovenia § 11 ods. 1 a 2 vzťahujú primerane.“.

10. V § 11 ods. 1 písm. c) sa slovo „platný“ vypúšťa a  za slová „verejný kľúč“ sa

 vkladajú slová „z platného kvalifikovaného certifikátu“.

11. V § 11 ods. 1 písm. d) na konci pripájajú tieto slová „alebo platný identifikátor ním

 akceptovanej podpisovej politiky zo zoznamu podľa § 4a ods. 4“

12. V § 11 ods. 2 písm. b) sa na konci pripájajú tieto slová „platnej v čase jeho

 vytvorenia“.

13. V § 12 ods. 1 a 2 sa slovo „kvalifikovaný“ a  slovo „zaručený“ vo všetkých

 tvaroch vypúšťa.

14. Doterajšia príloha sa označuje ako prílohe č. 1, ktorá vrátane nadpisu znie:

**„Príloha č. 1
k vyhláške č. 537/2002 Z. z.**

**PODPISOVÉ SCHÉMY, ŠIFROVACIE ALGORITMY A ICH PARAMETRE**

**Podpisové schémy**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Podpisováschéma** | **Asymetrickýalgoritmus** | **Minimálneparametreasymetrickéhoalgoritmu** | **Algoritmus nagenerovaniekľúčov** | **Metóda nadoplnenie(padding)** | **Hašovaciafunkcia** |
| 001 | RSA | MinModLen=1020 | rsagen1 | emsa-pkcs-v1\_5, 2\_0, 2\_1 | SHA1 |
| 002 | RSA | MinModLen=1020 | rsagen1 | emsa-pss | SHA1 |
| 003 | RSA | MinModLen=1020 | rsagen1 | emsa-pkcs- v1\_5, 2\_0, 2\_1 | RIPEMD160 |
| 004 | RSA | MinModLen=1020 | rsagen1 | emsa-pss | RIPEMD160 |
| 005 | DSA | pMinLen=1024qMinLen=160 | dsagen1 |       - | SHA1 |
| 006 | ECDSA-Fp | qMinLen=160r0Min=10000MinClass=200 | ecgen1 |       - | SHA1 |
| 007 | ECDSA-F2m | qMinLen=160r0Min=10000MinClass=200 | ecgen2 |      - | SHA1 |
| 008 | ECGDSA-Fp | qMinLen=160r0Min=10000MinClass=200 | Ecgen1 |       - | SHA1 |
| 009 | ECGDSA-F2m | qMinLen=160r0Min=10000MinClass=200 | Ecgen2 |      - | SHA1 |

**Algoritmy na generovanie kľúčov**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Označeniegenerátora kľúčov** | **Používanéoznačenie** | **Asymetrickýalgoritmus** | **Metódagenerovanienáhodných čísel** | **Parametrenáhodného generátora** |
| 4.01 | rsagen1 | RSA | trueran | EntropyBits = 128 |
| 4.02 | dsagen1 | DSA | trueran alebopseuran(FIPS 186-2) | EntropyBits = 128aleboSeedLen = 128 |
| 4.03 | ecgen1 | ECDSA-FpaleboECGDSA-Fp | trueran alebopseuran | EntropyBits = 128aleboSeedLen = 128 |
| 4.04 | ecgen2 | ECDSA-F2maleboECGDSA-F2m | trueran alebopseuran | EntropyBits = 128aleboSeedLen = 128 |

**Metódy generovania náhodných čísel**

|  |  |  |
| --- | --- | --- |
| **Označenienáhodného generátora** | **Používané meno** | **Parametre náhodného generátora** |
| 5.01 | trueran | EntropyBits |
| 5.02 | pseuran | SeedLen |
| 5.03  | FIPS 186-2-31 | SeedLen |
| 5.04  | FIPS 186-2-32 | SeedLen |

**Hašovacie funkcie**

|  |  |  |
| --- | --- | --- |
| **Označenie hašovacej funkcie** | **Používané meno** | **Doba platnosti** |
| 2.01 | SHA1 | Do 31. 12. 2008 |
| 2.02 | RIPEMD160 | Do 31. 12. 2014 |
| 2.03 | SHA-256 | - |
| 2.04 | Whirlpool | - |

Asymetrický šifrový algoritmus RSA s parametrom MinModLen 1024 bitov je v podpisových schémach 1 až 4 možné používať len do 31. 12. 2008. Od 1. 1. 2009 musí byť v uvedených podpisových schémach použitý algoritmus RSA s parametrom MinModLen 2048.

Hašovaciu funkciu SHA1 v podpisových schémach 1, 2, 5, až 7 možno používať len do 31. 12. 2008. Po tomto termíne musí byť použitá hašovacia funkcia SHA-2 a vyššia.

Pri výbere algoritmov sa odporúča postupovať v súlade s ETSI TS 102 176-1: „Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms”.“.

15. Za prílohu č. 1 sa vkladá príloha č. 2, ktorá vrátane nadpisu znie:

**„Príloha č. 2
k vyhláške č. 537/2002 Z. z.**

**PODPISOVÁ POLITIKA**

1. podpisová politika sa zverejňuje vo formáte strojovo čitateľnom podľa ETSI TR 102 272 (Electronic Signatures and Infrastructures (ESI);ASN.1 format for signature policies ) alebo ETSI TR 102 038.
2. Schválená podpisová politika je publikovaná na stránke úradu nasledujúcich päť rokov po skončení doby platnosti politiky.
3. Zoznam schválených podpisových politík obsahuje identifikačné údaje podľa §4a ods. 4. všetkých schválených podpisových politík zverejnených podľa bodu 2.
4. Štruktúra podpisovej politiky je tvorená z obálky podpisovej politiky, údajov podpisovej politiky, pravidiel pre overenie podpisu.
5. Obálka podpisovej politiky obsahuje identifikátor hašovacieho algoritmu, údaje podpisovej politiky a nepovinný digitálny odtlačok údajov podpisovej politiky.
6. Údaje podpisovej politiky obsahujú najmä:

 6.1 Identifikátor podpisovej politiky (OID),

 6.2 Dátum vydania,

 6.3 Meno vydavateľa,

 6.4 Oblasť použitia,

 6.5 Pravidlá pre overenie podpisu, ktoré obsahujú najmä

 6.5.1 dobu platnosti,

 6.5.2 všeobecné záväzné pravidlá,

 6.5.3 špecifické záväzky, ktoré môžu dopĺňať všeobecné záväzné pravidlá na

 základe identifikácie cez objektový identifikátor ktorý podpisovateľ zahrnul

 do podpísaných atribútov podpisu. K uvedenému objektovému identifikátoru

 musí byť priradená textová informácia, ktorú musí aplikácia podpisovateľovi

 a overovateľovi zobraziť,

 6.6 Pravidlá pre podpisovateľa a overovateľa o povinnosti uvedenia a overenia

 atribútov podpisu a certifikátu,

 6.7 Pravidlá pre použitie certifikátov koreňových certifikačných autorít pre

 podpisovateľa a pre overenie časovej pečiatky s definovaním maximálnej doby,

 do ktorej budú zverejnené informácie o zrušení certifikátu,

6.8 Povolené algoritmy a minimálne dĺžky kľúčov.

1. Pravidlá pri určovaní platnosti schválenej podpisovej politiky a postupy schvaľovania a rušenia schválených podpisových politík zverejňuje úrad na svojej internetovej stránke..

**Čl. II**

Táto vyhláška nadobúda účinnosť 1. mája 2008.