32

VYHLÁŠKA
Národného bezpečnostného úradu

z 27. januára 2010,

ktorou sa mení a dopĺňa vyhláška Národného bezpečnostného úradu č. 135/2009 Z. z. o formáte a spôsobe vyhotovenia zaručeného elektronického podpisu, spôsobe zverejňovania verejného kľúča úradu, podmienkach platnosti pre zaručený elektronický podpis, 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 vyhotovení a overovaní elektronického podpisu a časovej pečiatky)

Národný bezpečnostný 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 v znení neskorších predpisov ustanovuje:

Čl. I

Vyhláška Národného bezpečnostného úradu č. 135/2009 Z. z. o formáte a spôsobe vyhotovenia zaručeného elektronického podpisu, spôsobe zverejňovania verejného kľúča úradu, podmienkach platnosti pre zaručený elektronický podpis, 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 vyhotovení a overovaní elektronického podpisu a časovej pečiatky) sa mení a dopĺňa takto:

1. V § 6 sa za slovo „podpisov“ vkladajú slová „a časových pečiatok“.

2. Za § 13 sa vkladá § 13a, ktorý vrátane nadpisu znie:

„§ 13a

Prechodné ustanovenie
k úprave účinnej od 1. februára 2010

Certifikované produkty pre zaručený elektronický podpis využívajúce podpisové schémy s algoritmom RSA s parametrom MinModLen 1024 bitov a certifikované produkty využívajúce hašovaciu funkciu SHA1 uvedené v prílohe č. 1, ktoré bolo možné používať do 31. decembra 2009, možno používať do 31. decembra 2010.“.

3. Príloha č. 1 vrátane nadpisu znie:

**„Príloha č. 1
k vyhláške č. 135/2009 Z. z.**

PODPISOVÉ SCHÉMY

Podpisová schéma je tvorená postupnosťou označení uvedených v tejto prílohe, oddelených bodkočiarkou, kde ako prvé sa uvádza označenie podpisového algoritmu.[4])

Hašovacie funkcie

Označenie hašovacej funkcie	Používané meno	Doba platnosti
1.01	sha1	Do 31. 12. 2010
1.02	ripemd160	Do 31. 12. 2010
1.03	sha224	neurčená
1.04	sha256	neurčená
1.05	whirlpool	neurčená
1.06	sha384	neurčená
1.07	sha512	neurčená

Podpisové algoritmy

Označenie podpisového algoritmu	Podpisový algoritmus	Algoritmy generovania kľúčov	Podpisový algoritmus podľa minimálnej veľkosti parametrov a doba jeho použitia
2.01	rsa	rsagen1	MinModLen=1024, ErrProb= 2^{-80}, SeedEntropy/EntropyBits=80 – do 31. 12. 2010 MinModLen=2048, ErrProb= 2^{-100}, SeedEntropy/EntropyBits=100
2.02	dsa	dsagen1	pMinLen=1024, qMinLen= 160, ErrProb=2^{-80} , SeedEntropy/EntropyBits=80 – do 31. 12. 2010 pMinLen=2048, qMinLen=224, ErrProb=2^{-100}, SeedEntropy/EntropyBits=100
2.03	ecdsa-Fp	ecgen1	pMinLen=-, qMinLen=160, r0Min=104, MinClass=200, ErrProb=2^{-80}, SeedEntropy/EntropyBits=80 – do 31. 12. 2010 pMinLen=-, qMinLen=224, r0Min=104, MinClass=200, ErrProb=2^{-100}, SeedEntropy/EntropyBits=100
2.04	ecdsa-F2m	ecgen2	mMin=-, qMinLen=160, r0Min=104, MinClass=200, ErrProb=2^{-80}, SeedEntropy/EntropyBits=80 – do 31. 12. 2010 mMin=-, qMinLen=224, r0Min=104, MinClass=200, ErrProb=2^{-100}, SeedEntropy/EntropyBits=100
2.05	ecgdsa-Fp	ecgen1	pMinLen=-, qMinLen=160, r0Min=104, MinClass=200, ErrProb=2^{-80}, SeedEntropy/EntropyBits=80 – do 31. 12. 2010 pMinLen=-, qMinLen=224, r0Min=104, MinClass=200, ErrProb=2^{-100}, SeedEntropy/EntropyBits=100
2.06	ecgdsa-F2m	ecgen2	mMin=-, qMinLen=160, r0Min=104, MinClass=200, ErrProb=2^{-80}, SeedEntropy/EntropyBits=80 – do 31. 12. 2010 mMin=-, qMinLen=224, r0Min=104, MinClass=200, ErrProb=2^{-100}, SeedEntropy/EntropyBits=100

Algoritmy na generovanie kľúčových párov

Označenie generátora kľúčov	Používané označenie	Podpisový algoritmus	Metóda generovania náhodných čísel	Parametre náhodného generátora
3.01	rsagen1	rsa	trueran	EntropyBits
3.02	dsagen1	dsa	trueran alebo pseuran	EntropyBits alebo SeedEntropy
3.03	ecgen1	ecdsa-Fp, ecgdsa-Fp	trueran alebo pseuran	EntropyBits alebo SeedEntropy
3.04	ecgen2	ecdsa-F2m, ecgdsa-F2m	trueran alebo pseuran	EntropyBits alebo SeedEntropy

Metódy na doplnenie (padding)

Označenie metódy na doplnenie	Používané označenie	Metóda generovania náhodných čísel	Parametre náhodného generátora
4.01	emsa-pkcs1-v1.5	–	–
4.02	emsa-pkcs1-v2.1	–	–
4.03	emsa-pss	trueran/pseuran	MinSaltEntropy
4.04	iso9796ds2	trueran/pseuran	MinSaltEntropy
4.05	iso9796-din-rn	trueran/pseuran	MinSaltEntropy
4.06	iso9796ds3	–	–

Metódy generovania náhodných čísel

Označenie metódy generovania	Používané označenie	Parametre náhodného generátora
5.01	trueran	EntropyBits
5.02	pseuran	SeedEntropy

“.

Čl. II

Táto vyhláška nadobúda účinnosť 1. februára 2010.

František Blanárik v. r.