www.zbierka.sk Za obsah týchto stránok zodpovedá výhradne Forma, s.r.o.

537

VYHLÁŠKA
Národného bezpečnostného úradu

z 9. septembra 2002

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 vyhotovení 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 (ďalej len „zákon“) ustanovuje:

§ 1

Predmet úpravy

Táto vyhláška upravuje
a) formát a spôsob vyhotovenia zaručeného elektronického podpisu,
b) podrobnosti o podmienkach platnosti pre zaručený elektronický podpis, postup pri overovaní zaručeného elektronického podpisu a podmienky overenia platnosti zaručeného elektronického podpisu,
c) spôsob zverejňovania verejného kľúča úradu,
d) podpisové schémy, algoritmy a parametre týchto algoritmov na vyhotovovanie zaručeného elektronického podpisu,
e) formát a spôsob vyhotovovania časovej pečiatky,
f) požiadavky na vedenie dokumentácie časových pečiatok.

§ 2

Základné pojmy

Na účely tejto vyhlášky sa rozumie
a) podpisovou schémou jednoznačné určenie algoritmov na vyhotovenie a overenie zaručeného elektronického podpisu a ich parametrov,
b) schválenou podpisovou schémou podpisová schéma zo zoznamu podpisových schém schválených a zverejnených úradom,
c) hašovacou funkciou matematická transformácia, ktorá digitálnym dokumentom rozličnej dĺžky priradí také čísla vopred ustanovenej nenulovej pevnej dĺžky, že umožňujú overiť integritu digitálneho dokumentu, z ktorého boli odvodené transformáciou a nemožno z nich spätne odvodiť digitálny dokument,
d) schválenou hašovacou funkciou hašovacia funkcia uvedená v zozname schválených podpisových schém uvedených v prílohe,
e) digitálnym odtlačkom dokumentu číslo vypočítané z dokumentu pomocou hašovacej funkcie,
f) digitálnym podpisom elektronického dokumentu výsledok transformácie digitálneho odtlačku daného elektronického dokumentu pomocou algoritmu na vyhotovenie elektronického podpisu a súkromného kľúča podpisujúceho,
g) identifikátorom podpisovej politiky údaj jednoznačne určujúci danú podpisovú politiku,
h) referenčným časom čas, ktorý poskytuje niektoré z referenčných pracovísk,
i) vydavateľom časovej pečiatky (ďalej len „vydavateľ“) akreditovaná certifikačná autorita poskytujúca službu časových pečiatok,
j) spoliehajúcou sa stranou prijímateľ časovej pečiatky spoliehajúci sa na jej presnosť.

§ 3

Formáty zaručeného elektronického podpisu

(1) Zaručený elektronický podpis má formát
a) bez časovej pečiatky,
b) s časovou pečiatkou,
c) s úplnou informáciou na overenie platnosti,
d) archívny alebo
e) kombinácie formátov podľa písmen a) až d).

(2) Zaručený elektronický podpis bez časovej pečiatky obsahuje
a) identifikátor podpisovej politiky použitej pri vyhotovení a overovaní daného zaručeného elektronického podpisu,
b) podpisové údaje, ktoré podpisujúci zahrnul do zaručeného elektronického podpisu (napríklad miesto a čas vyhotovenia daného elektronického podpisu, meno fyzickej osoby podpisujúcej za právnickú osobu a pod.),
c) digitálny podpis, ktorý bol vyhotovený na základe
   1. digitálneho odtlačku podpisovaného dokumentu,
   2. identifikátora podpisovej politiky,
   3. údajov, ktoré podpisujúci zahrnul do elektronického podpisu.

(3) Zaručený elektronický podpis s časovou pečiatkou má formu zaručeného elektronického podpisu, ku ktorému je pripojená alebo s ním inak logicky spojená časová pečiatka vyhotovená na základe daného zaručeného elektronického podpisu postupom ustanoveným v § 7.

© Forma, s.r.o.

www.zbierka.sk Za obsah týchto stránok zodpovedá výhradne Forma, s.r.o.

(4) Zaručený elektronický podpis s úplnou informáciou na overenie platnosti má formu zaručeného elektronického podpisu s časovou pečiatkou, ku ktorému sú pripojené úplné informácie o všetkých kvalifikovaných certifikátoch verejných kľúčov potrebných na overenie platnosti daného zaručeného elektronického podpisu, ako aj úplné informácie o zoznamoch zrušených kvalifikovaných certifikátov alebo informácie o stave kvalifikovaných certifikátov, ktoré sú rozhodujúce na overenie platnosti daného zaručeného elektronického podpisu.

(5) Archívny zaručený elektronický podpis má formu zaručeného elektronického podpisu s časovou pečiatkou, ku ktorému sú pripojené všetky údaje potrebné na overenie daného archívneho zaručeného elektronického podpisu podľa § 11 ods. 1. Na údaje potrebné na overenie daného archívneho zaručeného elektronického podpisu je vyhotovená časová pečiatka, ktorá je k nim pripojená.

(6) Úrad zverejňuje platné formáty zaručených elektronických podpisov a ich formálne špecifikácie na svojej internetovej stránke.

§ 4

Podpisová politika

(1) Podpisová politika je súbor pravidiel upravujúcich vyhotovovanie a overovanie zaručených elektronických podpisov. Zaručený elektronický podpis vyhotovuje podpisovateľ v súlade s určenou podpisovou politikou. Platnosť zaručeného elektronického podpisu overuje overovateľ vzhľadom na podpisovú politiku, ktorá bola použitá pri jeho vyhotovení.

(2) Subjekt, ktorý prijíma dokumenty podpísané zaručeným elektronickým podpisom, určí podpisovú politiku, ktorú akceptuje.

(3) Podpisovateľ a overovateľ zaručeného elektronického podpisu použijú tú istú podpisovú politiku.

(4) Obsah a štruktúra podpisovej politiky je zverejnená na internetovej stránke úradu.

§ 5

Vyhotovenie zaručeného elektronického podpisu

(1) Zaručený elektronický podpis elektronického dokumentu podpisovateľ vyhotovuje pomocou bezpečného zariadenia na vyhotovenie elektronického podpisu[1]) na základe elektronického dokumentu a súkromného kľúča podpisovateľa podľa niektorej zo schválených podpisových schém podľa § 6.

(2) Zaručený elektronický podpis s časovou pečiatkou podpisovateľ vyhotovuje na základe zaručeného elektronického podpisu prostredníctvom vydavateľa časových pečiatok tak, že časovú pečiatku vydanú akreditovanou certifikačnou autoritou na daný zaručený elektronický podpis pripojí k zaručenému elektronickému podpisu alebo ju logicky spojí so zaručeným elektronickým podpisom, na ktorý bola daná časová pečiatka vydaná.

(3) Zaručený elektronický podpis s úplnou informáciou na overenie platnosti vyhotovuje podpisovateľ po vyhotovení zaručeného elektronického podpisu s časovou pečiatkou alebo overovateľ zaručeného elektronického podpisu s časovou pečiatkou tak, že k zaručenému elektronickému podpisu s časovou pečiatkou pripojí referencie o všetkých údajoch potrebných na overenie daného zaručeného elektronického podpisu s časovou pečiatkou podľa § 11.

(4) Archívny elektronický podpis podpisovateľ vyhotovuje po vyhotovení zaručeného elektronického podpisu s časovou pečiatkou tak, že k zaručenému elektronickému podpisu s časovou pečiatkou pripojí všetky údaje potrebné na overenie daného zaručeného elektronického podpisu s časovou pečiatkou podľa § 7 a časovú pečiatku, ktorá bola na tieto údaje vydaná.

§ 6

Podpisové schémy na vyhotovovanie zaručeného elektronického podpisu a časovej pečiatky

Zoznam schválených podpisových schém, schválených algoritmov a parametrov schválených algoritmov na vyhotovovanie zaručených elektronických podpisov je uvedený v prílohe.

§ 7

Vyhotovenie a overenie časovej pečiatky

(1) Politika časových pečiatok je súbor pravidiel, ktoré ustanovujú použiteľnosť časovej pečiatky určitého okruhu používateľov časových pečiatok a triedy aplikácií so spoločnými bezpečnostnými požiadavkami.[1]) Politiku časových pečiatok vytvárajú používatelia časových pečiatok a vydavatelia časových pečiatok.

(2) Právnická osoba alebo fyzická osoba, ktorá žiada o vyhotovenie časovej pečiatky (ďalej len „žiadateľ“), zašle vydavateľovi časových pečiatok žiadosť o vyhotovenie časovej pečiatky. Žiadosť obsahuje digitálny odtlačok dokumentu, na ktorý sa má vyhotoviť časová pečiatka, vytvorený pomocou schválenej hašovacej funkcie.

(3) Ak je žiadosť v súlade s požiadavkami ustanovenými v odseku 2 a nie sú prekážky na vyhotovenie časovej pečiatky zo strany vydavateľa podľa § 9 ods. 4, vydavateľ pomocou bezpečného zariadenia na vyhotovovanie časových pečiatok a zdroja času vyhotoví časovú pečiatku na predložený digitálny odtlačok dokumentu a do času ustanovenému politikou časových pečiatok ju pošle žiadateľovi.

(4) Ak žiadosť o vyhotovenie časovej pečiatky nespĺňa požiadavky ustanovené v odseku 2 alebo u vydavateľa vznikli prekážky vyhotovenia časovej pečiatky podľa § 9 ods. 4, vydavateľ časovú pečiatku na predložený digitálny odtlačok dokumentu nevyhotoví

[1]) 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).

© Forma, s.r.o.

www.zbierka.sk Za obsah týchto stránok zodpovedá výhradne Forma, s.r.o.

a o tejto skutočnosti a jej príčine informuje žiadateľa do času ustanovenému politikou časových pečiatok.

(5) Overenie platnosti časovej pečiatky vykonáva spoliehajúca sa strana na základe časovej pečiatky a dokumentu, na ktorý bola daná časová pečiatka vyhotovená, a politiky časových pečiatok, ktorá sa na danú časovú pečiatku vzťahuje. Časová pečiatka je platná, ak

a) je v súlade s použitou politikou časových pečiatok,
b) zaručený elektronický podpis časovej pečiatky vydavateľa je platný podľa § 11 ods. 1 a 2.

(6) Formát žiadosti o vyhotovenie časovej pečiatky, formát časovej pečiatky a formát odpovede na žiadosť o vyhotovenie časovej pečiatky je zverejnený na internetovej stránke úradu.

§ 8

Požiadavky na zdroj časových údajov pre časovú pečiatku

Zdroj časových údajov, ktorý používa vydavateľ na vyhotovovanie časovej pečiatky, musí spĺňať nasledujúce požiadavky

a) zdroj časových údajov je synchronizovaný s referenčným zdrojom času s deklarovanou presnosťou,
b) kalibrácia zdroja časových údajov je udržiavaná tak, aby bolo zaručené, že nenastane odchýlka nad rámec deklarovanej presnosti,
c) zdroj časových údajov je chránený pred nebezpečenstvom, ktoré by mohlo mať za následok nezistiteľné zmeny zdroja časových údajov vedúce k odchýlke nad rámec kalibrácie,
d) zabezpečená je detekcia prípadov, keď sa časový údaj, ktorý má byť uvedený v časovej pečiatke, odchyľuje od synchronizácie s referenčným zdrojom času; o tom musí vydavateľ informovať spoliehajúce sa strany,
e) vydavateľ vykonáva synchronizáciu zdroja časových údajov v prípade vydania opravnej sekundy na základe oznámenia správcu referenčného času,
f) vydavateľ vykonáva zmenu, pri ktorej nastaví opravnú sekundu v poslednej minúte dňa, na ktorý je zmena plánovaná; o presnom čase, s deklarovanou presnosťou uskutočnenia takejto zmeny, vydavateľ vyhotovuje záznam.

§ 9

Požiadavky na časové údaje pre časovú pečiatku

(1) Vydavateľ vyhotovuje časové pečiatky spoľahlivým spôsobom. Časové pečiatky musia obsahovať správny časový údaj.

(2) Na vydávanie časových pečiatok vydavateľ používa aspoň jeden zdroj času poskytujúci spoľahlivé časové údaje, ktorý spĺňa požiadavky uvedené v § 8.

(3) Časový údaj, ktorý obsahuje časová pečiatka, je preukázateľne odvodený aspoň z jednej hodnoty referenčného času.

(4) Ak zdroj časových údajov nedosahuje potrebnú presnosť, t. j. odchyľuje sa od referenčného zdroja času viac, ako je určené v prevádzkovom poriadku vydavateľa časových pečiatok, vydavateľ časovú pečiatku nevydá.

§ 10

Dokumentácia časových pečiatok

(1) Všetky informácie o poskytovaní služby vydávania časových pečiatok sú zaznamenávané a uchovávané v súlade s politikou časových pečiatok.

(2) Pri vydávaní časových pečiatok vydavateľ uchováva

a) zoznam vydavateľom vyhotovených časových pečiatok, pričom časová pečiatka je od jej vyhotovenia uchovaná v lehote ustanovenej politikou časových pečiatok, ktorú vydavateľ používa,
b) záznamy o mimoriadnych udalostiach v systéme používanom v manažmente časových pečiatok,
c) záznamy o dôležitých udalostiach v prostredí vydavateľa časových pečiatok, manažmente kryptografických kľúčov a v synchronizácii zdrojov času vrátane presných časových údajov.

§ 11

Overenie platnosti zaručeného elektronického podpisu

(1) Na overenie platnosti zaručeného elektronického podpisu overovateľ používa

a) elektronický dokument, pre ktorý bol zaručený elektronický podpis vyhotovený,
b) zaručený elektronický podpis elektronického dokumentu,
c) platný verejný kľúč prislúchajúci k súkromnému kľúču, pomocou ktorého bol zaručený elektronický podpis vyhotovený,
d) podpisovú politiku, ktorej identifikátor je uvedený v zaručenom elektronickom podpise.

(2) Na overenie platnosti zaručeného elektronického podpisu elektronického dokumentu na základe údajov uvedených v odseku 1 a algoritmov uvedených v podpisovej schéme použitej na vyhotovenie zaručeného elektronického podpisu je potrebné zistiť, či

a) je platný digitálny podpis obsiahnutý v zaručenom elektronickom podpise,
b) zaručený elektronický podpis elektronického dokumentu bol vyhotovený podľa určenej podpisovej politiky.

(3) Platnosť zaručeného elektronického podpisu nemožno overiť, ak overovateľ nemá údaje uvedené v odseku 1.

(4) Overenie zaručeného elektronického podpisu s časovou pečiatkou pozostáva z overenia

a) platnosti zaručeného elektronického podpisu podľa odsekov 1 a 2,
b) platnosti časovej pečiatky zaručeného elektronického podpisu podľa § 7 ods. 5.

(5) Overenie zaručeného elektronického podpisu s úplnou informáciou na overenie platnosti pozostáva z overenia

a) dostupnosti a úplnosti informácií na overenie zaručeného elektronického podpisu,

© Forma, s.r.o.

www.zbierka.sk Za obsah týchto stránok zodpovedá výhradne Forma, s.r.o.

b) platnosti zaručeného elektronického podpisu s časovou pečiatkou podľa odseku 4.

(6) Overenie platnosti archívneho zaručeného elektronického podpisu spočíva v overení
a) platnosti časovej pečiatky podľa § 7 ods. 5, ktorá bola vyhotovená na základe údajov podľa odseku 1,
b) úplnosti informácií na overenie zaručeného elektronického podpisu,
c) platnosti zaručeného elektronického podpisu s časovou pečiatkou podľa odseku 4.

§ 12

Verejný kľúč úradu

(1) Verejný kľúč úradu je verejný kľúč prislúchajúci k súkromnému kľúču úradu. Pomocou súkromného kľúča úradu úrad
a) vyhotovuje zaručený elektronický podpis kvalifikovaných certifikátov verejných kľúčov akreditovaných certifikačných autorít,
b) vyhotovuje zaručený elektronický podpis kvalifikovaného certifikátu vlastného verejného kľúča,
c) vyhotovuje zaručený elektronický podpis úradom vydávaného zoznamu zrušených kvalifikovaných certifikátov.

(2) Úrad zverejňuje svoj verejný kľúč uverejnením kvalifikovaného certifikátu verejného kľúča úradu v tlači a na internetovej stránke úradu. Úrad môže zverejniť svoj verejný kľúč aj iným spôsobom.

(3) Úrad vydáva nový verejný kľúč úradu 30 dní pred uplynutím platnosti aktuálneho verejného kľúča úradu a zverejňuje ho spôsobom uvedeným v odseku 2.

§ 13

Účinnosť

Táto vyhláška nadobúda účinnosť 1. októbra 2002.

Ján Mojžiš v. r.

© Forma, s.r.o.

www.zbierka.sk

Za obsah týchto stránok zodpovedá výhradne Forma, s.r.o.

Príloha
k vyhláške č. 537/2002 Z. z.

PODPISOVÉ SCHÉMY, ŠIFROVACIE ALGORITMY A ICH PARAMETRE

Podpisové schémy

Podpisová schéma	Asymetrický algoritmus	Minimálne parametre asymetrického algoritmu	Algoritmus na generovanie kľúčov	Metóda na doplnenie (padding)	Hašovacia funkcia
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=1024 qMinLen=160	dsagen1	-	SHA1
006	ECDSA-Fq	qMinLen=160 r0Min=10000 MinClass=200	ecgen1	-	SHA1
007	ECDSA-F2m	qMinLen=160 r0Min=10000 MinClass=200	ecgen1	-	SHA1

Algoritmy na generovanie kľúčov

Označenie generátora kľúčov	Používané označenie	Asymetrický algoritmus	Metóda generovania náhodných čísel	Parametre náhodného generátora
4.01	rsagen1	RSA	trueran	EntropyBits = 128
4.02	dsagen1	DSA	trueran alebo pseuran (FIPS 186-2)	EntropyBits = 128 alebo SeedLen = 128
4.03	ecgen1	ECDSA-Fq alebo ECDSA-F2m	trueran alebo pseudoran	EntropyBits = 128 alebo SeedLen = 128

© Forma, s.r.o.

www.zbierka.sk
Za obsah týchto stránok zodpovedá výhradne Forma, s.r.o.

Metódy generovania náhodných čísel

Označenie náhodného 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**
2.01	SHA1
2.02	RIPEMD160

© Forma, s.r.o.