ZBIERKA ZÁKONOV
SLOVENSKEJ REPUBLIKY

Ročník 2009

Vyhlásené: 8. 4. 2009 Vyhlásená verzia v Zbierke zákonov Slovenskej republiky

Obsah tohto dokumentu má informatívny charakter.

135

VYHLÁŠKA

Národného bezpečnostného úradu

z 26. marca 2009

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 (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,

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

§ 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 č. 1,

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 je objektový identifikátor jednoznačne určujúci podpisovú politiku, ktorý prideľuje úrad; formát a tvorba objektového identifikátora je ustanovená v medzinárodnom štandardizačnom dokumente,[1])

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,

k) vydavateľom podpisovej politiky subjekt, ktorý prostredníctvom podpisovej politiky definuje špecifické, technické a procedurálne pravidlá na vytvorenie a overenie zaručeného elektronického podpisu.

§ 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 podobne),

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 ods. 2 a 3 a v § 8.

(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 certifikátoch verejných kľúčov potrebných na overenie platnosti daného zaručeného elektronického podpisu, ako aj úplné informácie o zoznamoch zrušených certifikátov alebo informácie o stave 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. 5. 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 webovej stránke.

§ 4
Podpisová politika

(1) Podpisová politika je súbor pravidiel upravujúcich vyhotovovanie a overovanie zaručených elektronických podpisov.

(2) Subjekt, ktorý prijíma dokumenty podpísané zaručeným elektronickým podpisom, určí podpisovú politiku, ktorú akceptuje. Zaručený elektronický podpis vyhotovuje podpisovateľ v súlade s určenou podpisovou politikou. Platnosť zaručeného elektronického podpisu overuje overovateľ vzhľadom na podpisovú politiku, ktorá sa použila pri jeho vyhotovení.

(3) Ak orgán verejnej moci nemá vydanú vlastnú podpisovú politiku, pri overovaní zaručeného elektronického podpisu dokumentov prijatých od orgánov verejnej moci a pri overovaní zaručeného elektronického podpisu dokumentov doručených orgánom verejnej moci použije úradom vydanú podpisovú politiku.

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

(5) Formát, obsahové náležitosti a štruktúra podpisovej politiky sú uvedené v prílohe č. 2.

(6) Ak podpisová politika spĺňa požiadavky podľa odseku 5, zverejňuje sa na webovej stránke úradu a zaraďuje sa do zoznamu schválených podpisových politík. Podpisová politika sa zverejňuje v strojovo spracovateľnom formáte podľa medzinárodných štandardizačných dokumentov.[2])

(7) Zoznam schválených podpisových politík obsahuje názov súboru podpisovej politiky, hašovaciu funkciu, digitálny odtlačok súboru podpisovej politiky, dátum platnosti, objektový identifikátor a oblasť použitia podpisovej politiky.

§ 5
Vyhotovenie zaručeného elektronického podpisu

(1) Zaručený elektronický podpis elektronického dokumentu podpisovateľ vyhotovuje pomocou bezpečného zariadenia na vyhotovenie elektronického podpisu[3]) 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 § 11 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 č. 1.

§ 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.[3]) 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 ustanoveného 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 a o tejto skutočnosti a jej príčine informuje žiadateľa do času ustanoveného 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) elektronický podpis časovej pečiatky vydavateľa je platný.

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

§ 8
Požiadavky na zdroj časových údajov pre časovú pečiatku

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

a) zdroj časových údajov je synchronizovaný s referenčným zdrojom času s deklarovanou presnosťou,

b) kalibrácia zdroja časových údajov sa udržiava 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 sa zaznamenávajú a uchovávajú 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) Zaručený elektronický podpis je platný, ak

a) je platný digitálny podpis obsiahnutý v zaručenom elektronickom podpise,

b) zaručený elektronický podpis elektronického dokumentu bol vytvorený podľa určenej podpisovej politiky, platnej v čase jeho vytvorenia,

c) sú platné všetky certifikáty v certifikačnej ceste.

(2) Zaručený elektronický podpis s časovou pečiatkou je platný, ak je jednoznačne preukázateľná

a) platnosť zaručeného elektronického podpisu podľa odsekov 1 a 5 k času z platnej časovej pečiatky zaručeného elektronického podpisu,

b) platnosť časovej pečiatky zaručeného elektronického podpisu podľa § 7 ods. 5.

(3) Zaručený elektronický podpis s úplnou informáciou na overenie platnosti je platný, ak

a) sú dostupné a úplné informácie na overenie zaručeného elektronického podpisu podľa odseku 5,

b) je platný zaručený elektronický podpis s časovou pečiatkou podľa odseku 2.

(4) Archívny zaručený elektronický podpis je platný, ak je jednoznačne preukázateľná

a) platnosť časovej pečiatky podľa § 7 ods. 5, ktorá bola vyhotovená na základe údajov podľa odsekov 1 a 5,

b) úplnosť informácií na overenie zaručeného elektronického podpisu,

c) platnosť zaručeného elektronického podpisu s časovou pečiatkou podľa odseku 2.

(5) Na overenie platnosti zaručeného elektronického podpisu overovateľ používa

a) elektronický dokument, pre ktorý sa zaručený elektronický podpis vyhotovil,

b) zaručený elektronický podpis elektronického dokumentu,

c) verejný kľúč z platného kvalifikovaného certifikátu prislúchajúci k súkromnému kľúču, ktorého pomocou sa zaručený elektronický podpis vyhotovil,

d) podpisovú politiku, ktorej objektový identifikátor je uvedený v zaručenom elektronickom podpise alebo platný objektový identifikátor ním akceptovanej podpisovej politiky zo zoznamu podľa § 4 ods. 7,

e) platné verejné kľúče prislúchajúce k súkromným kľúčom, ktorých pomocou sa vyhotovili podpisy certifikátov a zoznamov certifikátov v certifikačnej ceste,

f) zoznamy zrušených certifikátov pre všetky certifikáty v certifikačnej ceste, prípadne informáciu o stave certifikátov v certifikačnej ceste získanú z potvrdenia o existencii a platnosti certifikátu.

§ 12
Verejný kľúč úradu

(1) Verejný kľúč úradu je verejný kľúč prislúchajúci k súkromnému kľúču úradu. Pomocou súkromného kľúča úradu úrad

a) vyhotovuje elektronický podpis certifikátov verejných kľúčov akreditovaných certifikačných autorít,

b) vyhotovuje elektronický podpis certifikátu vlastného verejného kľúča,

c) vyhotovuje elektronický podpis úradom vydávaného zoznamu zrušených certifikátov.

(2) Úrad zverejňuje svoj verejný kľúč uverejnením certifikátu verejného kľúča úradu v tlači a na webovej 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
Prechodné ustanovenia

(1) Certifikované produkty pre zaručený elektronický podpis využívajúce podpisové schémy s asymetrickým šifrovým algoritmom RSA s parametrom MinModLen 1024 bitov alebo nižším a certifikované produkty využívajúce hašovaciu funkciu SHA1 možno používať do uplynutia doby platnosti certifikátu produktu, najdlhšie však do 31. decembra 2009.

(2) Produkty pre zaručený elektronický podpis využívajúce algoritmus RSA certifikované po 1. januári 2009 musia používať algoritmus RSA s parametrom MinModLen 2048. Produkty pre zaručený elektronický podpis využívajúce algoritmus SHA certifikované po 1. januári 2009 musia použiť hašovaciu funkciu z rady SHA-2 alebo inú z odporúčaných hašovacích funkcií s dobou platnosti dlhšou ako do 31. decembra 2009.

(3) Certifikáty pre poskytovanie akreditovaných certifikačných služieb využívajúce hašovaciu funkciu SHA1 a algoritmus RSA s parametrom MinModLen nižším ako 2048 bitov možno používať na overovanie do 31. decembra 2010.

(4) Pri poskytovaní akreditovaných certifikačných služieb pre vydávanie zoznamu zrušených certifikátov a potvrdzovanie existencie a platnosti kvalifikovaných certifikátov možno používať hašovaciu funkciu SHA1 a algoritmus RSA s parametrom MinModLen nižším ako 2048 bitov do 31. decembra 2010.

(5) Pri výbere algoritmov sa odporúča postupovať v súlade s medzinárodným štandardizačným dokumentom.[4])

§ 14
Zrušovacie ustanovenie

Zrušuje sa 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 vyhotovení a overovaní elektronického podpisu a časovej pečiatky).

§ 15
Záverečné ustanovenie

Táto vyhláška bola prijatá v súlade s príslušným právnym aktom Európskych spoločenstiev[5]) pod číslom notifikácie 2008/0528/SK.

§ 16
Účinnosť

Táto vyhláška nadobúda účinnosť dňom vyhlásenia.

František Blanárik v. r.

Príloha č. 1
k vyhláške č. 135/2009 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=1 020	rsagen1	emsa-pkcs-v1_5, 2_0, 2_1	SHA1
002	RSA	MinModLen=1 020	rsagen1	emsa-pss	SHA1
003	RSA	MinModLen=1 020	rsagen1	emsa-pkcs-v1_5, 2_0, 2_1	RIPEMD160
004	RSA	MinModLen=1 020	rsagen1	emsa-pss	RIPEMD160
005	DSA	pMinLen=1 024 qMinLen=160	dsagen1	–	SHA1
006	ECDSA-Fp	qMinLen=160 r0Min=10 000 MinClass=200	ecgen1	–	SHA1
007	ECDSA-F2m	qMinLen=160 r0Min=10 000 MinClass=200	ecgen2	–	SHA1
008	ECGDSA-Fp	qMinLen=160 r0Min=10 000 MinClass=200	ecgen1	–	SHA1
009	ECGDSA-F2m	qMinLen=160 r0Min=10 000 MinClass=200	ecgen2	–	SHA1

Algoritmy na generovanie kľúčov

Označenie generátora kľúčov	**Používané označenie**	**Asymetrický algoritmus**	**Metóda generovanie 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-Fp alebo ECGDSA-Fp	trueran alebo pseuran	EntropyBits = 128 alebo SeedLen = 128
4.04	ecgen2	ECDSA-F2m alebo ECGDSA-F2m	trueran alebo pseuran	EntropyBits = 128 alebo SeedLen = 128

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**	**Doba platnosti**
2.01	SHA1	Do 31. 12. 2009
2.02	RIPEMD160	Do 31. 12. 2014
2.03	SHA-224	-
2.04	SHA-256	-
2.05	SHA-384	-
2.06	SHA-512	-
2.07	Whirlpool	Do 31. 12. 2014

Príloha č. 2
k vyhláške č. 135/2009 Z. z.

PODPISOVÁ POLITIKA

1. Štruktúra podpisovej politiky je tvorená z obálky podpisovej politiky, údajov podpisovej politiky, pravidiel pre overenie podpisu.
2. Obálka podpisovej politiky obsahuje identifikátor hašovacieho algoritmu, údaje podpisovej politiky a nepovinný digitálny odtlačok údajov podpisovej politiky.
3. Údaje podpisovej politiky obsahujú najmä
   - 3.1 Objektový identifikátor (OID),
   - 3.2 Dátum vydania,
   - 3.3 Meno vydavateľa,
   - 3.4 Oblasť použitia,
   - 3.5 Pravidlá pre overenie podpisu, ktoré obsahujú najmä
     - 3.5.1 Dobu platnosti,
     - 3.5.2 Všeobecné záväzné pravidlá,
     - 3.5.3 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.
   - 3.6 Pravidlá pre podpisovateľa a overovateľa o povinnosti uvedenia a overenia atribútov podpisu a certifikátu,
   - 3.7 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,
   - 3.8 Povolené algoritmy a minimálne dĺžky kľúčov.

1) ISO/IEC 6523.

2) ETSI TR 102 272 Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies [Elektronické podpisy a infraštruktúry (ESI). Formát ASN.1 pre podpisové politiky] alebo ETSI TR 102 038 TC Security – Electronic Signatures and Infrastructures (ESI). XML format for signature policies [TC Bezpečnosť – Elektronické podpisy a infraštruktúry (ESI). Formát XML pre podpisové politiky].

3) 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).

4) ETSI TS 102 176-1: Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms [Elektronické podpisy a infraštruktúry (ESI). Algoritmy a parametre pre bezpečné elektronické podpisy. Časť 1: Hašovacie funkcie a asymetrické algoritmy].

5) Smernica Európskeho Parlamentu a Rady 98/34/ES o postupe pri poskytovaní informácií v oblasti technických noriem a predpisov (Ú. v. ES L 204, 21. 7. 1998; Mimoriadne vydanie Ú. v. EÚ kap. 3/zv. 20) v platnom znení.

Vydavateľ Zbierky zákonov Slovenskej republiky, správca obsahu a prevádzkovateľ právneho a informačného portálu Slov-Lex dostupného na webovom sídle www.slov-lex.sk je
Ministerstvo spravodlivosti Slovenskej republiky, Župné námestie 13, 813 11 Bratislava,
tel.: 02 888 91 137, fax: 02/52442853, e-mail: helpdesk@slov-lex.sk.