

ZBIERKA  **ZÁKONOV**
SLOVENSKEJ REPUBLIKY

Ročník 2009

Vyhlásené: 8. 4. 2009 Časová verzia predpisu účinná od: 15. 3.2014 do: 17.10.2016

Obsah tohto dokumentu má informatívny charakter.

131

VYHLÁŠKA

Národného bezpečnostného úradu

z 26. marca 2009

**o formáte, obsahu a správe certifikátov a kvalifikovaných certifikátov
a formáte, periodicite a spôsobe vydávania zoznamu zrušených
kvalifikovaných certifikátov (o certifikátoch a kvalifikovaných
certifikátoch)**

Národný bezpečnostný úrad (ďalej len „úrad“) podľa § 6 ods. 10, § 7 ods. 8, § 8 ods. 6, § 14 ods. 3 písm. f) a § 27 zákona č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení zákona č. 214/2008 Z. z. (ďalej len „zákon“) ustanovuje:

§ 1

Predmet úpravy

Táto vyhláška upravuje

- a) formát a obsah certifikátu na správu a kvalifikovaného certifikátu,
- b) podrobnosti o správe certifikátov,
- c) formát zoznamu zrušených certifikátov,
- d) periodicitu vydávania zoznamu zrušených certifikátov,
- e) spôsob vydávania zoznamu zrušených certifikátov,
- f) formát a obsah potvrdenia existencie a platnosti certifikátov,
- g) formát a obsah zoznamu platných kvalifikovaných systémových certifikátov.

§ 2

Základné pojmy

Na účely tejto vyhlášky sa rozumie

- a) certifikátom na správu certifikát, ktorý slúži na overenie platnosti kvalifikovaných certifikátov – certifikátov úradu, certifikátov akreditovaných certifikačných autorít, certifikátov časových pečiatok, certifikátov na overenie potvrdenia existencie a platnosti certifikátov¹⁾ a certifikátov na overenie zoznamu zrušených certifikátov,²⁾
- b) digitálnym odtlačkom údajov číslo vypočítané z údajov pomocou hašovacej funkcie.³⁾

§ 3

Formát a obsah certifikátu na správu a kvalifikovaného certifikátu

(1) Formát certifikátu na správu a kvalifikovaného certifikátu vymedzuje usporiadanie a spôsob zápisu údajov v certifikáte na správu a v kvalifikovanom certifikáte. Schválené formáty týchto certifikátov úrad zverejňuje na svojom webovom sídle.

(2) Obsahom certifikátu na správu a kvalifikovaného certifikátu sú údaje uvedené v tele certifikátu podľa § 6 a 7 zákona.

(3) Identifikačné údaje uvedené v kvalifikovanom certifikáte musia obsahovať

- a) identifikačné údaje vydavateľa certifikátu zhodné s identifikačnými údajmi držiteľa certifikátu uvedenými v certifikáte vydanom príslušnej akreditovanej certifikačnej autorite na príslušný verejný kľúč,
- b) obchodné meno a sídlo akreditovanej certifikačnej autority.

(4) Identifikačné údaje držiteľa kvalifikovaného certifikátu vydaného podľa § 7 ods. 1 zákona sú

- a) meno a priezvisko alebo pseudonym a
- b) doplňujúci identifikátor^{3a)} zabezpečujúci jednoznačnosť identifikačných údajov držiteľa kvalifikovaného certifikátu.

(5) Identifikačnými údajmi držiteľa kvalifikovaného certifikátu vydaného podľa § 7 ods. 3 zákona sú:

- a) meno a priezvisko a
- b) doplňujúci identifikátor^{3a)} zabezpečujúci jednoznačnosť identifikačných údajov držiteľa kvalifikovaného certifikátu.

(6) Identifikačnými údajmi držiteľa kvalifikovaného certifikátu vydaného podľa § 7 ods. 8 zákona sú:

- a) názov orgánu verejnej moci alebo právnickej osoby a
- b) doplňujúci identifikátor^{3a)} zabezpečujúci jednoznačnosť identifikačných údajov držiteľa kvalifikovaného certifikátu.

(7) Identifikačnými údajmi mandanta v kvalifikovanom certifikáte vydanom podľa § 7 ods. 3 zákona sú:

- a) názov orgánu verejnej moci alebo právnickej osoby alebo meno a priezvisko fyzickej osoby, za ktorú alebo v mene ktorej mandatár koná, a
- b) doplňujúci identifikátor^{3a)} zabezpečujúci jednoznačnosť identifikačných údajov mandanta.

(8) Certifikát na správu a kvalifikovaný certifikát obsahuje identifikátor certifikačného poriadku akreditovaných certifikačných služieb, ktorého hodnotu zverejňuje úrad v schválených formátoch certifikátov. Identifikátor certifikačného poriadku akreditovaných certifikačných služieb sa smie použiť iba v certifikáte na správu a v kvalifikovaných certifikátoch.

§ 4

Podrobnosti o správe kvalifikovaných certifikátov

(1) Pred vydaním kvalifikovaného certifikátu vydaného podľa § 7 ods. 1 zákona akreditovaná certifikačná autorita alebo registračná autorita, ktorá koná v jej mene, vykonáva kontrolu, či

- a) osobné údaje žiadateľa uvedené v žiadosti o vydanie kvalifikovaného certifikátu súhlasia s údajmi v predloženom preukaze totožnosti, ak ide o prvé vydanie kvalifikovaného certifikátu,
- b) osobné údaje žiadateľa uvedené v žiadosti o vydanie kvalifikovaného certifikátu súhlasia s údajmi v dokumentácii získanej pri predošlom registračnom procese tohto žiadateľa, ak ide o následné vydanie kvalifikovaného certifikátu a žiadosť o vydanie kvalifikovaného certifikátu bola podaná v podobe elektronického dokumentu podpísaného zaručeným elektronickým

podpisom overeným kľúčom z kvalifikovaného certifikátu predošlého registračného procesu tohto žiadateľa,

- c) identifikačné údaje, ktoré sa majú uviesť ako identifikačné údaje držiteľa certifikátu, súhlasia s údajmi uvedenými v žiadosti o vydanie kvalifikovaného certifikátu,
- d) žiadateľ o vydanie kvalifikovaného certifikátu disponuje súkromným kľúčom prislúchajúcim k verejnému kľúču, ktorý sa má uviesť v kvalifikovanom certifikáte ako verejný kľúč držiteľa certifikátu,
- e) verejný kľúč, ktorý sa má uviesť v kvalifikovanom certifikáte ako verejný kľúč držiteľa kvalifikovaného certifikátu a ktorý je zhodný s verejným kľúčom držiteľa kvalifikovaného certifikátu uvedeným v inom kvalifikovanom certifikáte, spĺňa bezpečnostné požiadavky pre periódu použitia v kvalifikovanom certifikáte a či súkromný kľúč prislúchajúci k tomuto verejnému kľúču nebol kompromitovaný,^{3b)}
- f) verejný kľúč, ktorý sa má uviesť v kvalifikovanom certifikáte ako verejný kľúč držiteľa certifikátu, a súkromný kľúč prislúchajúci k tomuto verejnému kľúču sú generované a uložené na bezpečnom zariadení na vyhotovenie elektronického podpisu.

(2) Pred vydaním kvalifikovaného certifikátu podľa § 7 ods. 3 zákona akreditovaná certifikačná autorita alebo registračná autorita, ktorá koná v jej mene, vykonáva kontrolu, či

- a) osobné údaje žiadateľa uvedené v žiadosti o vydanie kvalifikovaného certifikátu súhlasia s údajmi v predloženom preukaze totožnosti,
- b) osobné údaje žiadateľa uvedené v žiadosti o vydanie kvalifikovaného certifikátu súhlasia s údajmi v platných dokladoch podľa § 10a ods. 2 písm. b) zákona,
- c) identifikačné údaje, ktoré sa majú uviesť ako identifikačné údaje držiteľa kvalifikovaného certifikátu, súhlasia s údajmi uvedenými v žiadosti o vydanie kvalifikovaného certifikátu,
- d) žiadateľ o vydanie kvalifikovaného certifikátu disponuje súkromným kľúčom prislúchajúcim k verejnému kľúču, ktorý sa má uviesť v kvalifikovanom certifikáte ako verejný kľúč držiteľa kvalifikovaného certifikátu,
- e) verejný kľúč, ktorý sa má uviesť v kvalifikovanom certifikáte ako verejný kľúč držiteľa kvalifikovaného certifikátu, nie je zhodný s verejným kľúčom držiteľa kvalifikovaného certifikátu uvedeným v inom kvalifikovanom certifikáte vydanom tou istou akreditovanou certifikačnou autoritou,
- f) verejný kľúč, ktorý sa má uviesť v kvalifikovanom certifikáte ako verejný kľúč držiteľa kvalifikovaného certifikátu, a súkromný kľúč prislúchajúci k tomuto verejnému kľúču sú generované a uložené na bezpečnom zariadení na vyhotovenie elektronického podpisu.

(3) Pred vydaním kvalifikovaného certifikátu podľa § 7 ods. 8 zákona akreditovaná certifikačná autorita alebo registračná autorita, ktorá koná v jej mene, vykonáva kontrolu, či

- a) údaje uvedené v dokumentoch k žiadosti o vydanie kvalifikovaného certifikátu súhlasia s údajmi v predloženom preukaze totožnosti osoby oprávnenej konať v mene žiadateľa,
- b) identifikačné údaje, ktoré sa majú uviesť ako identifikačné údaje držiteľa kvalifikovaného certifikátu, súhlasia s údajmi uvedenými v žiadosti o vydanie kvalifikovaného certifikátu,
- c) verejný kľúč, ktorý sa má uviesť v kvalifikovanom certifikáte ako verejný kľúč držiteľa kvalifikovaného certifikátu, nie je zhodný s verejným kľúčom držiteľa kvalifikovaného certifikátu uvedeným v inom certifikáte zverejnenom v zozname platných kvalifikovaných systémových certifikátov podľa § 8a,
- d) verejný kľúč, ktorý sa má uviesť v kvalifikovanom certifikáte ako verejný kľúč držiteľa kvalifikovaného certifikátu, a súkromný kľúč prislúchajúci k tomuto verejnému kľúču sú generované na bezpečnom zariadení počas vydávania kvalifikovaného certifikátu.

(4) Akreditovaná certifikačná autorita zasiela mesačne úradu zoznam ňou vydaných kvalifikovaných certifikátov a ňou vydaných certifikátov na správu. Zoznam týchto certifikátov obsahuje sériové číslo certifikátu, meno vydavateľa, údaje držiteľa certifikátu, dátum platnosti certifikátu a iné. Technické podrobnosti o spôsobe doručenia, formáte a obsahu zoznamu vydaných certifikátov zverejňuje úrad na svojom webovom sídle.

§ 5

Formát zoznamu zrušených certifikátov

(1) Formát zoznamu zrušených certifikátov vymedzuje usporiadanie a spôsob zápisu údajov v zozname. Zoznam obsahuje údaje vydavateľa zoznamu, dátum a čas vydania zoznamu, sériové číslo zrušeného certifikátu, dátum a čas zrušenia certifikátu a iné.

(2) Identifikačné údaje vydavateľa certifikátov uvedené v zozname zrušených certifikátov musia byť zhodné s identifikačnými údajmi vydavateľa uvedenými v certifikátoch, ktorých identifikačné čísla sa v tomto zozname zrušených certifikátov nachádzajú.

(3) Identifikačné údaje vydavateľa certifikátov uvedené v zozname zrušených certifikátov musia byť zhodné s identifikačnými údajmi držiteľa certifikátu uvedenými v certifikáte na verejný kľúč prislúchajúci k súkromnému kľuču použitému na vytvorenie elektronického podpisu zoznamu zrušených certifikátov.

§ 6

Periodicita vydávania zoznamu zrušených certifikátov

Zoznamy zrušených certifikátov sa vydávajú s periódou maximálne 24 hodín a zároveň tak, aby od prijatia žiadosti o zrušenie certifikátu do zverejnenia prvého zoznamu zrušených certifikátov, ktorý obsahuje jeho číslo, neuplynulo viac ako 24 hodín.

§ 7

Spôsob vydávania zoznamu zrušených certifikátov

(1) Akreditovaná certifikačná autorita vydá nový zoznam zrušených certifikátov tak, že v zozname identifikačných čísel certifikátov, ktoré boli zrušené, uvedie všetky identifikačné čísla certifikátov, ktoré boli uvedené v predchádzajúcom zozname zrušených certifikátov spolu s dátumami a časmi ich zrušenia, a pridá identifikačné čísla všetkých certifikátov, pre ktoré nastali skutočnosti podľa § 15 zákona; dátum a čas ich zrušenia je v intervale od času vydania predchádzajúceho zoznamu zrušených certifikátov do času vydania zoznamu zrušených certifikátov. Identifikačné číslo zrušeného certifikátu je v zozname zrušených certifikátov uvádzané minimálne do uplynutia pôvodnej doby platnosti certifikátu. Pred ukončením pôvodnej doby platnosti zrušený certifikát musí byť najmenej raz uvedený v zozname zrušených certifikátov.

(2) Akreditovaná certifikačná autorita zverejňuje aktuálny zoznam zrušených certifikátov a všetky predchádzajúce zoznamy zrušených certifikátov na svojom webovom sídle.

(3) Akreditovaná certifikačná autorita mesačne zasiela úradu každý ňou vydaný zoznam zrušených certifikátov za uvedené obdobie. Technické podrobnosti o spôsobe doručenia vydaného zoznamu zrušených certifikátov, formáte a obsahu zoznamu zverejňuje úrad na svojom webovom sídle.

§ 8**Formát a obsah potvrdenia existencie a platnosti certifikátov**

(1) Akreditovaná certifikačná autorita prijíma žiadosti o potvrdenie existencie a platnosti certifikátov vo forme nepodpísaného zoznamu identifikátorov certifikátov. Identifikátory certifikátov sa skladajú z týchto položiek:

- a) identifikátora použitej hašovacej funkcie,
- b) digitálneho odtlačku z mena vydavateľa certifikátu,
- c) digitálneho odtlačku z verejného kľúča vydavateľa certifikátu,
- d) sériového čísla certifikátu.

(2) Akreditovaná certifikačná autorita potvrdzuje existenciu a platnosť certifikátov potvrdením vo forme elektronického dokumentu.

(3) Potvrdenie sa skladá z tela potvrdenia, z elektronického podpisu tela potvrdenia a zoznamu certifikátov na overenie podpisu tela potvrdenia.

(4) Telo potvrdenia je elektronický dokument, ktorý obsahuje

- a) identifikačné údaje vydavateľa potvrdenia, ktorý spravuje informácie o certifikátoch,
- b) dátum a čas vydania potvrdenia,
- c) zoznam samotných potvrdení na jeden certifikát, ktorý obsahuje
 1. identifikátor certifikátu definovaný v odseku 1,
 2. stav certifikátu, ktorý je platný, zrušený alebo neznámy,
 3. dátum a čas, v ktorom bol stav certifikátu známy a správny,
 4. rozšírenie samotného potvrdenia a pozitívne vyhlásenie, ktoré obsahuje identifikátor hašovacej funkcie a digitálny odtlačok z certifikátu, ktorého stav sa nachádza v odpovedi, a iné.

(5) Elektronický podpis tela potvrdenia je vyhotovený vydavateľom potvrdenia, ktorý spravuje informácie pre tieto certifikáty, použitím na to určeného súkromného kľúča.

(6) Potvrdenie existencie a platnosti certifikátov je zoznam identifikátorov certifikátov, ktorým vydavateľ potvrdenia, ktorý spravuje informácie o týchto certifikátoch, oznamuje existenciu alebo predčasné ukončenie ich platnosti. Potvrdenie spĺňa požiadavky podľa odsekov 1 až 5 a

- a) je vydané akreditovanou certifikačnou autoritou alebo úradom,
- b) elektronický podpis tela potvrdenia bol vyhotovený použitím súkromného kľúča určeného na tento účel,
- c) na verejný kľúč patriaci k súkromnému kľúču podľa písmena b) vydala akreditovaná certifikačná autorita alebo úrad certifikát.

(7) Technické podrobnosti o formáte a spôsobe vydávania potvrdenia existencie a platnosti certifikátov úrad zverejňuje na svojom webovom sídle.

§ 8a**Zoznam platných kvalifikovaných systémových certifikátov**

Zoznam platných kvalifikovaných systémových certifikátov má formát obsahujúci najmä sériové číslo certifikátu, údaje o vydavateľovi, údaje o držiteľovi, údaje o platnosti certifikátu a jeho odtlačok.

§ 9**Zrušovacie ustanovenie**

Zrušuje sa vyhláška Národného bezpečnostného úradu č. 538/2002 Z. z. o formáte a obsahu kvalifikovaného certifikátu, o správe kvalifikovaných certifikátov a o formáte, periodicite a spôsobe vydávania zoznamu zrušených kvalifikovaných certifikátov (o kvalifikovaných certifikátoch).

§ 10**Záverčné ustanovenia**

(1) Touto vyhláškou sa preberajú právne akty Európskych spoločenstiev a Európskej únie uvedené v prílohe.

(2) Táto vyhláška bola prijatá v súlade s príslušným právnym aktom Európskych spoločenstiev⁴⁾ pod číslom notifikácie 2008/0529/SK.

§ 11**Účinnosť**

Táto vyhláška nadobúda účinnosť dňom vyhlásenia.

František Blanárik v. r.

**Príloha
k vyhláske č. 131/2009 Z. z.****ZOZNAM PREBERANÝCH PRÁVNÝCH AKTOV EURÓPSKYCH SPOLOČENSTIEV A EURÓPSKEJ
ÚNIE**

Smernica Európskeho parlamentu a Rady 1999/93/ES z 13. decembra 1999 o rámci spoločenstva pre elektronické podpisy (Ú. v. ES L 13, 19. 1. 2000; Mimoriadne vydanie Ú. v. EÚ, kap. 13/zv. 24).

- 1) IETF RFC 6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol.
- 2) ITU-T RECOMMENDATION X.509 | ISO/IEC 9594-8 Information technology - open systems interconnection - the directory: public key and attribute certificate frameworks, IETF RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
- 3) 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 na bezpečné elektronické podpisy. Časť 1: Hašovacie funkcie a asymetrické algoritmy].
 - 3a) § 3 písm. j) zákona č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente).
 - 3b) Príloha č. 1 k vyhláske 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) v znení vyhlásky č. 32/2010 Z. z.
Kapitola 7.3.2, ETSI EN 319 411-2 V1.1.1 (2013-01): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates [Elektronické podpisy a infraštruktúry (ESI). Požiadavky politiky a bezpečnostné požiadavky pre poskytovateľov dôveryhodných služieb vydávajúcich certifikáty. Časť 2: Požiadavky politiky pre certifikačné authority vydávajúce kvalifikované certifikáty].
- 4) 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.

