60

VYHLÁŠKA
Národného bezpečnostného úradu

z 10. marca 2014,

ktorou sa mení a dopĺňa vyhláška Národného bezpečnostného úradu č. 131/2009 Z. z. o formáte, obsahu a správe certifikátov a kvalifikovaných certifikátov a formáte, periodicite a spôsobe vydávania zoznamu zrušených kvalifikovaných certifikátov (o certifikátoch a kvalifikovaných certifikátoch) v znení vyhlášky č. 323/2012 Z. z.

Národný bezpečnostný úrad podľa § 6 ods. 11, § 7 ods. 9, § 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 neskorších predpisov ustanovuje:

Čl. I

Vyhláška Národného bezpečnostného úradu č. 131/2009 Z. z. o formáte, obsahu a správe certifikátov a kvalifikovaných certifikátov a formáte, periodicite a spôsobe vydávania zoznamu zrušených kvalifikovaných certifikátov (o certifikátoch a kvalifikovaných certifikátoch) v znení vyhlášky č. 323/2012 Z. z. sa mení a dopĺňa takto:

1. V úvodnej vete sa slová „§ 6 ods. 10, § 7 ods. 8 a § 8 ods. 6“ nahrádzajú slovami „§ 6 ods. 10, § 7 ods. 8, § 8 ods. 6, § 14 ods. 3 písm. f) a § 27“.

2. § 1 sa dopĺňa písmenom g), ktoré znie:
„g) formát a obsah zoznamu platných kvalifikovaných systémových certifikátov.“.

3. V § 2 písmeno a) znie:
„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 certifikátov[1]) a certifikátov na overenie zoznamu zrušených certifikátov,[2])“.

Poznámky pod čiarou k odkazom 1 a 2 znejú:
„[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.“.

4. V § 3 ods. 4 a § 4 ods. 1 uvádzacej vete sa za slovo „certifikátu“ vkladajú slová „vydaného podľa § 7 ods. 1 zákona“.

5. V § 3 ods. 4 písm. b) sa nad slovo „identifikátor“ umiestňuje odkaz 3a a za slovo „držiteľa“ sa vkladá slovo „kvalifikovaného“.

Poznámka pod čiarou k odkazu 3a znie:
„[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).“.

6. V § 3 sa za odsek 4 vkladajú nové odseky 5 až 7, ktoré znejú:
„(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.“.

Doterajšie odseky 5 a 6 sa označujú ako odseky 8 a 9.

7. V § 3 ods. 8 druhej vete sa vypúšťajú slová „fyzickej osoby“.

8. V § 3 sa vypúšťa odsek 9.

9. V § 4 ods. 1 písm. b) sa na konci pripájajú tieto slová: „overeným kľúčom z kvalifikovaného certifikátu predošlého registračného procesu tohto žiadateľa“.

10. V § 4 ods. 1 písmeno e) znie:
„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])“.

Poznámka pod čiarou k odkazu 3b znie:
„[3b]) Príloha č. 1 k vyhláške 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 elektro-

nický 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 vyhlášky 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 autority vydávajúce kvalifikované certifikáty].“.

11. V § 4 ods. 1 písm. f) sa za slovo „generované“ vkladajú slová „a uložené“ a slová „pre vytvorenie“ sa nahrádzajú slovami „na vyhotovenie“.

12. V § 4 sa za odsek 1 vkladajú nové odseky 2 a 3, ktoré znejú:

„(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.“.

Doterajší odsek 2 sa označuje ako odsek 4.

13. Za § 8 sa vkladá § 8a, ktorý vrátane nadpisu znie:

„§ 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.“.

Čl. II

Táto vyhláška nadobúda účinnosť 15. marca 2014.

Jozef Magala v. r.