**Návrh**

**Vyhláška**

**Národného bezpečnostného úradu**

**z.........................2008,**

**ktorou sa mení a dopĺňa 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)**

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

**Čl. I**

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) sa mení a dopĺňa takto:

1. V § 1 písm. a) sa za slová „formát a obsah“ vkladajú slová „certifikátu na správu kvalifikovaného certifikátu a“.
2. V § 1 písm. b) až c) sa slovo „kvalifikovaných“ vypúšťa.
3. § 1 sa dopĺňa písmenom f), ktoré znie:

„f) formát a obsah potvrdenia existencie a platnosti certifikátov.“.

1. Za § 1 sa vkladá § 1a, ktorý vrátane nadpisu znie:

„§ 1a

Základné pojmy

Na účely tejto vyhlášky sa rozumie

1. certifikátom na správu kvalifikovaného certifikátu (ďalej len „certifikát“) certifikát slúžiaci na overenie platnosti kvalifikovaného certifikátu - certifikát úradu, certifikát akreditovanej certifikačnej autority, certifikát časovej pečiatky, certifikát na overenie potvrdenia existencie a platnosti certifikátov1) a certifikát na overenie zoznamu zrušených certifikátov,2)
2. 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,
3. digitálnym odtlačkom údajov číslo vypočítané z údajov pomocou hašovacej funkcie.“.

Poznámky pod čiarou k odkazom 1 a 2 znejú:

„1) RFC 2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol.

2) ITU-T RECOMMENDATION X.509 (08/2005) | ISO/IEC 9594-8.“.

1. § 2 vrátane nadpisu znie:

„§2

Formát a obsah certifikátu a kvalifikovaného certifikátu

(1) Formát certifikátu a kvalifikovaného certifikátu vymedzuje usporiadanie a spôsob zápisu údajov v certifikáte a kvalifikovanom certifikáte. Schválené formáty týchto certifikátov úrad zverejňuje na svojej internetovej stránke.

(2) Obsahom certifikátu 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 certifikátu uvedené v kvalifikovanom certifikáte musia obsahovať

a) meno a priezvisko alebo pseudonym a

b) doplňujúci identifikátor zabezpečujúci jednoznačnosť identifikačných údajov

držiteľa certifikátu.

     (5) Identifikačné údaje držiteľa kvalifikovaného certifikátu musia jednoznačne identifikovať fyzickú osobu spomedzi ostatných, ktorým kvalifikovaný certifikát vydala tá istá akreditovaná certifikačná autorita.

(6) Identifikačné údaje držiteľa certifikátu vydaného akreditovanou certifikačnou autoritou alebo úradom musia jednoznačne identifikovať akreditovanú certifikačnú autoritu spomedzi ostatných, ktorým certifikát vydal úrad.

(7) Certifikát 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 a kvalifikovaných certifikátoch fyzickej osoby.“.

1. V § 3 písm. d) sa slová „vydanom tou istou akreditovanou certifikačnou autoritou“ vypúšťajú.

1. Doterajší text § 3 sa označuje ako odsek 1 a dopĺňa sa odsekom 2, ktorý znie:

„(2) Akreditovaná certifikačná autorita zasiela úradu zoznam ňou vydaných kvalifikovaných certifikátov, ktoré držiteľ kvalifikovaného certifikátu povolil zverejniť a ňou vydaných certifikátov. Spôsob doručenia, formát a obsah zoznamu vydaných certifikátov 1) zverejňuje úrad na svojej stránke.“.

1. V § 4 a 5 sa slovo „kvalifikovaný“ vo všetkých tvaroch vypúšťa..
2. § 6 vrátane nadpisu znie:

„§ 6

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 (aktuálneho) zoznamu zrušených certifikátov. Identifikačné číslo zrušeného certifikátu musí byť v zozname zrušených certifikátov uvádzané až do uplynutia pôvodnej doby platnosti certifikátu. Pred ukončením pôvodnej doby platnosti zrušený certifikát musí byť v zozname zrušených certifikátov uvedený minimálne raz po uplynutí pôvodnej doby platnosti.

(2) Akreditovaná certifikačná autorita zverejňuje aktuálny zoznam zrušených certifikátov a všetky predchádzajúce zoznamy zrušených certifikátov na svojej internetovej stránke.

(3) Akreditovaná certifikačná autorita zasiela úradu každý zoznam zrušených certifikátov, ktorý obsahuje nový záznam o zrušení certifikátu. Spôsob doručenia vydaného zoznamu zrušených certifikátov, formát a obsah zoznamu zverejňuje úrad na svojej internetovej stránke.“.

1. Za § 6 sa vkladajú § 6a a 6b, ktoré vrátane nadpisov znejú:

„§ 6a

Formát a obsah potvrdenia existencie a platnosti certifikátov

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

a) identifikátor hašovacej funkcie,

b) digitálny odtlačok z mena vydavateľa certifikátu,

c) digitálny odtlačok z verejného kľúča vydavateľa certifikátu,

d) sériové číslo 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 najmä

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 najmä

1. identifikátor certifikátu definovaný v odseku 1,

2. stav certifikátu, ktorý je buď platný, zrušený alebo neznámy,

3. dátum a čas, v ktorom bol stav certifikátu známy a správny,

4. rozšírenie samotného potvrdenia a  pozitívne prehlásenie, ktoré obsahuje najmä

identifikátor hašovacej funkcie a digitálny odtlačok z certifikátu, ktorého stav sa

nachádza v odpovedi (odkaz na zahraničný dokument: ISIS - MTT

SPECIFICATION Part 4 Private OCSP Extensions CertHash (Positive

Statement)).

(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 certifikátu je zoznam identifikátorov certifikátov, ktorým vydavateľ potvrdenia, ktorý spravuje informácie o týchto certifikátoch, oznamuje existenciu alebo predčasné ukončenie ich platnosti. Potvrdenie musí spĺňať požiadavky podľa odsekov 1 až 6 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) Formát a spôsob vydávania potvrdenia existencie a platnosti certifikátov úrad zverejňuje na svojej internetovej stránke v dokumente „Schválené formáty zoznamu zrušených certifikátov.

§ 6b

Záverečné ustanovenie

Touto vyhláškou sa preberá právny akt Európskych spoločenstiev uvedený v prílohe.“.

11. Vyhláška sa dopĺňa prílohou, ktorá znie:

„Príloha k vyhláške č. 538/2002 Z. z.

Zoznam preberaných právnych aktov Európskych spoločenstiev:

Smernica Európskeho parlamentu a  Rady 1999/93/ES z  13.decembra 1999 o rámci

spoločenstva pre elektronické podpisy (Mimoriadne vydanie Ú. v. EÚ, 13/zv. 24).“.

**Čl. II**

Táto vyhláška nadobúda účinnosť 1. mája 2008