

## **Stanovisko k § 13 a k § 13a vyhlášky Národného bezpečnostného úradu č. 135/2009 Z. z. o vyhotovení a overovaní elektronického podpisu a časovej pečiatky.**

Pre jednoznačnú interpretáciu a správnu aplikáciu vyššie uvedených prechodných ustanovení vyhlášky Národného bezpečnostného úradu č. 135/2009 Z. z. o vyhotovení a overovaní elektronického podpisu a časovej pečiatky (ďalej len „vyhláška“) v praxi, zaujíma Národný bezpečnostný úrad, ako vecný gestor pre problematiku elektronického podpisu v Slovenskej republike, nasledovné stanovisko.

*Podľa § 13 ods. 1 vyhlášky certifikované produkty pre zaručený elektronický podpis, využívajúce podpisové schémy s algoritmom RSA s parametrom MinModLen 1024 bitov alebo nižším a certifikované produkty, využívajúce hašovaciu funkciu SHA1, je možné používať do uplynutia doby platnosti certifikátu produktu, najdlhšie však do 31. decembra 2009.*

*Uvedené ustanovenie bolo upravené novelou vyhlášky NBÚ č. 32/2010 Z. z., ktorá nadobudla účinnosť dňa 1. februára 2010. V znení § 13a predmetnej novely sa upravuje doba používania vyššie uvedených produktov od 1. februára 2010 do 31. decembra 2010.*

Certifikované produkty pre zaručený elektronický podpis, ktorých sa predmetné ustanovenie týka sú :

- a) produkty na uchovávanie súkromných kľúčov na vyhotovenie zaručeného elektronického podpisu určené pre podpisovateľa (bezpečné zariadenia na vyhotovovanie elektronického podpisu, tzv. Secure Signature-Creation Devices (SSCD)),
- b) softvérové produkty pre vyhotovovanie a overovanie elektronického podpisu (Signature Creation and Verification Application (SCVA)).

Ak produkty uvedené v písmene a) pri vyhotovení a overovaní zaručeného elektronického podpisu používajú algoritmus RSA s dĺžkou kľúča do 1024 bitov, **možno ich od 1. februára 2010 ďalej používať pre vyhotovenie zaručeného elektronického podpisu, najdlhšie však do 31. decembra 2010.**

Ak produkty uvedené v písmene b) pri vytváraní a overovaní zaručeného elektronického podpisu využívajú hašovaciu funkciu SHA1, **možno ich od 1. februára 2010 ďalej používať pre vyhotovenie zaručeného elektronického podpisu, najdlhšie však do 31. decembra 2010.**

Elektronický podpis vyhotovený v období od 1. januára 2010 do 1. februára 2010, teda do schválenia novely vyhlášky, za použitia algoritmu RSA dĺžkou kľúča menšou ako 2048 bitov a hašovacej funkcie SHA1 nemožno považovať za zaručený elektronický podpis.

*Podľa § 13 ods. 2 vyhlášky 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.*

Uvedené ustanovenie upravuje proces certifikácie a používanie vyššie uvedených produktov pre zaručený elektronický podpis. Produkty, ktoré sa certifikujú po 1. januári 2009, ak sa certifikujú pre algoritmus RSA, musia umožniť použitie RSA s dĺžkou kľúča minimálne 2048 bitov. Produkty

musia podporovať hašovaciú funkciu z rady odporúčaných hašovacích funkcií s dobou platnosti dlhšou ako do 31. decembra 2010 podľa prílohy č.1 k vyhláske.

V dôsledku uvedeného – ak držiteľ kvalifikovaného certifikátu má vydaný kvalifikovaný certifikát na RSA kľúč s dĺžkou 1024 bitov, môže tento používať do ukončenia doby platnosti certifikátu, najdlhšie však do 31. decembra 2010. Akreditované certifikačné autority (ACA) sú povinné podľa § 14 zákona o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov informovať o tejto skutočnosti dotknutých držiteľov certifikátov. Po termíne 31. decembra 2010 na vyhotovenie zaručeného elektronického podpisu za použitia podpisovej schémy RSA/SHA musí byť použitý kľúč s minimálnou dĺžkou 2048 bitov a niektorá z hašovacích funkcií SHA224, SHA256, SHA384, SHA512.

Doba platnosti parametrov podpisových algoritmov a hašovacích funkcií je uvedená v prílohe č.1 k vyhláske, Podpisové schémy, v jednotlivých tabuľkách. Podľa § 6 vyhlásky sa podpisové schémy uvedené v prílohe č. 1 k vyhláske vzťahujú aj na vyhotovenie časovej pečiatky pre zaručený elektronický podpis.

*Podľa § 13 ods. 3 vyhlásky certifikáty pre poskytovanie akreditovaných certifikačných služieb využívajúce hašovaciú funkciu SHA1 a algoritmus RSA s parametrom MinModLen nižším ako 2048 bitov možno používať na overovanie do 31. decembra 2010.*

Uvedené ustanovenie upravuje prechodné obdobie používania certifikátov akreditovanej certifikačnej autority, ktoré používa pre poskytovanie certifikačných služieb. Súkromný kľúč kľúčového páru, na ktorého verejnú časť bol Národným bezpečnostným úradom vydaný certifikát ACA, už nie je možné využívať na vydávanie nových kvalifikovaných certifikátov ani certifikátov na správu. Možno ho však používať pre overenie vydaných kvalifikovaných certifikátov a certifikátov na správu. **Kvalifikovaný certifikát fyzickej osoby, ktorý vydavateľ (ACA) podpísal za použitia SHA1 je možné pre vyhotovenie zaručeného elektronického podpisu používať do uplynutia doby jeho platnosti, najdlhšie však do 31. decembra 2010.**