386

VYHLÁŠKA

ze dne 17. prosince 2015

o náležitostech kryptografických klíčů a autentizačního certifikátu

Ministerstvo vnitra stanoví podle § 26 písm. g) zákona č. 328/1999 Sb., o občanských průkazech, ve znění zákona č. 559/2004 Sb., zákona č. 227/2009 Sb., zákona č. 424/2010 Sb. a zákona č. 318/2015 Sb.:

§ 1

Kryptografické klíče odpovídající autentizačnímu certifikátu, který lze zapsat do kontaktního elektronického čipu občanského průkazu, se vytvářejí a užívají s využitím algoritmu RSA s délkou klíče 2048 bitů v souladu se standardem PKCS #1 v2.2: RSA Cryptography Standard ze dne 27. října 2012.

§ 2

Autentizační certifikát, který lze zapsat do kontaktního elektronického čipu občanského průkazu, obsahuje

a) jméno, popřípadě jména, a příjmení držitele občanského průkazu,
b) zvláštní znaky držitele občanského průkazu, vyžaduje-li to účel autentizačního certifikátu,
c) obchodní firmu nebo název nebo jméno, popřípadě jména, a příjmení subjektu, který autentizační certifikát vydal, a stát, ve kterém je usazen,
d) číslo autentizačního certifikátu unikátní u subjektu, který autentizační certifikát vydal, a
e) údaje o počátku a konci platnosti autentizačního certifikátu.

§ 3

(1) Autentizační certifikát, který lze zapsat do kontaktního elektronického čipu občanského průkazu, se vytváří a užívá s využitím hashovací funkce SHA-2 s délkou hashe 256 bitů, 384 bitů nebo 512 bitů v souladu se standardem FIPS PUB 180-4: Secure Hash Standard ze srpna 2015 a s využitím algoritmu RSA s délkou klíče 2048 bitů v souladu se standardem PKCS #1 v2.2: RSA Cryptography Standard ze dne 27. října 2012.

(2) Autentizační certifikát, který lze zapsat do kontaktního elektronického čipu občanského průkazu, se vytváří, ukládá a užívá ve formátu stanoveném v souladu se standardem RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile z května 2008.

(3) Kryptografické klíče a žádost o vydání autentizačního certifikátu se generují prostřednictvím kontaktního elektronického čipu občanského průkazu.

§ 4

Účinnost

Tato vyhláška nabývá účinnosti dnem 1. ledna 2016.

Ministr:

Chovanec v. r.