N á v r h

VYHLÁŠKA

ze dne……2015

o náležitostech kryptografických klíčů a autentizačního certifikátu a o bezpečnostních zásadách pro užití autentizačního certifikátu

Ministerstvo vnitra stanoví podle § 26 písm. g) zákona č. 328/1999 Sb., o občanských průkazech, ve znění zákona č. …/2015 Sb.:

§ 1

Náležitosti kryptografických klíčů

Soukromý kryptografický klíč a veřejný kryptografický klíč, které lze zapsat do kontaktního elektronického čipu,

a) se vytvářejí a užívají s využitím některého z algoritmů uvedených v bodu I přílohy k této vyhlášce a
b) se vytvářejí, ukládají a používají ve formátu stanoveném standardem uvedeným v bodu III přílohy k této vyhlášce.

§ 2

Náležitosti autentizačního certifikátu

Autentizační certifikát, který lze zapsat do kontaktního elektronického čipu,

a) se vytváří a užívá s využitím hashovací funkce uvedené v bodu II přílohy k této vyhlášce a s využitím některého z algoritmů uvedených v bodu I přílohy k této vyhlášce,
b) se vytváří, ukládá a používá ve formátu stanoveném standardem uvedeným v bodu III přílohy k této vyhlášce a
c) obsahuje
    1. jméno, popřípadě jména, a příjmení držitele občanského průkazu,
    2. obchodní firmu nebo název akreditovaného poskytovatele certifikačních služeb, který autentizační certifikát vydal, jedná-li se o právnickou osobu, nebo jméno, popřípadě jména, příjmení, případně odlišující dodatek, jedná-li se o fyzickou osobu, a stát, ve kterém je akreditovaný poskytovatel certifikačních služeb usazen,
    3. číslo autentizačního certifikátu unikátní u daného akreditovaného poskytovatele certifikačních služeb a
    4. údaje o počátku a konci platnosti autentizačního certifikátu.

§ 3

Bezpečnostní zásady pro užití autentizačního certifikátu

Užití autentizačního certifikátu se řídí bezpečnostními zásadami uvedenými v certifikační politice, kterou akreditovaný poskytovatel certifikačních služeb vede v souladu se standardem uvedeným v bodu III přílohy k této vyhlášce a zveřejňuje ji způsobem umožňujícím dálkový přístup.

§ 4

Tato vyhláška byla oznámena v souladu se směrnicí Evropského parlamentu a Rady 98/34/ES ze dne 22. června 1998 o postupu při poskytování informací v oblasti norem a technických předpisů a předpisů pro služby informační společnosti, ve znění směrnice 98/48/ES.

§ 5

Účinnost

Tato vyhláška nabývá účinnosti dnem 1. ledna 2016.

Příloha k vyhlášce č. …/2015 Sb.

Seznam algoritmů, hashovacích funkcí a standardů

I. Algoritmy
   a) RSA 2048 bitů (RFC 3447)
   b) DSA (FIPS PUB 186-2)
   c) ECDSA-Fp (ANSI X9.62)
   d) ECDSA-F2m (ANSI X9.62)

II. Hashovací funkce
   SHA-2 – 256, 384, 512 bitů (FIPS 180-2)

III. Standard
   ETSI TS 102 042 – Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates