269

VYHLÁŠKA

ze dne 16. srpna 2016

o způsobu tvorby podpisového kódu poplatníka a bezpečnostního kódu poplatníka

Ministerstvo financí stanoví podle § 19 odst. 3 zákona č. 112/2016 Sb., o evidenci tržeb:

§ 1

Způsob tvorby podpisového kódu poplatníka

(1) Podpisový kód poplatníka je tvořen podepsaným otiskem řetězce údajů o evidované tržbě a vyjádřen v kódování Base64 podle části A přílohy k této vyhlášce.

(2) Řetězcem údajů o evidované tržbě je posloupnost vybraných údajů o evidované tržbě uvedených v kódování UTF-8 podle části A přílohy k této vyhlášce ve tvaru, ve kterém jsou zasílány datovou zprávou, a oddělených svislým oddělovačem, kterým je znak s dekadickým kódem 124 v kódování Unicode podle části A přílohy k této vyhlášce.

(3) Vybranými údaji o evidované tržbě jsou v tomto pořadí:

a) daňové identifikační číslo poplatníka,
b) označení provozovny, ve které je tržba uskutečněna,
c) označení pokladního zařízení, na kterém je tržba evidována,
d) pořadové číslo účtenky,
e) datum a čas přijetí tržby nebo vystavení účtenky, pokud je vystavena dříve, a
f) celková částka tržby.

(4) K vytvoření otisku řetězce údajů o evidované tržbě se použije kryptografická hashovací funkce SHA-256 podle části B přílohy k této vyhlášce.

(5) Otisk řetězce údajů o evidované tržbě se podepíše podpisovým schématem RSASSA-PKCS1-v1_5 podle části C přílohy k této vyhlášce pomocí soukromého klíče, který náleží k používanému certifikátu pro evidenci tržeb platnému ke dni evidované tržby.

§ 2

Způsob tvorby bezpečnostního kódu poplatníka

(1) Bezpečnostní kód poplatníka je tvořen otiskem podpisového kódu poplatníka vyjádřeného v osmibitovém kódování podle části A přílohy k této vyhlášce a je vyjádřen v kódování Base16 podle části A přílohy k této vyhlášce ve formě 5 skupin po 8 znacích oddělených pomlčkou, kterou je znak s dekadickým kódem 45 v kódování Unicode podle části A přílohy k této vyhlášce.

(2) K vytvoření otisku podpisového kódu poplatníka se použije kryptografická hashovací funkce SHA-1 podle části B přílohy k této vyhlášce.

§ 3

Účinnost

Tato vyhláška nabývá účinnosti dnem 1. prosince 2016.

Ministr:

Ing. **Babiš** v. r.

Příloha k vyhlášce č. 269/2016 Sb.

Část A – Kódování

Název kódování	Standard
Osmibitové kódování	[1]
Base16	[2]
Base64	[2]
UTF-8	[3]
Unicode	[4]

Standardy:

[1] RFC 1341 MIME (Multipurpose Internet Mail Extensions): Mechanisms for Specifying and Describing the Format of Internet Message Bodies: https://tools.ietf.org/html/rfc1341
[2] RFC 4648 The Base16, Base32, and Base64 Data Encodings: https://tools.ietf.org/html/rfc4648

[3] RFC 3629 UTF-8, a transformation format of ISO 10646: https://tools.ietf.org/html/rfc3629

[4] Standard Unicode verze 8.0: http://www.unicode.org/versions/Unicode8.0.0/

Část B – Kryptografické hashovací funkce

Název funkce	Standard
SHA-1	[1]
SHA-256	[2]

Standardy:

[1] RFC 3174 US Secure Hash Algorithm 1 (SHA1): https://tools.ietf.org/html/rfc3174

[2] RFC 4634 US Secure Hash Algorithms (SHA and HMAC-SHA): https://tools.ietf.org/html/rfc4634

Část C – Podpisové schéma

Název schématu	Standard
RSASSA-PKCS1-v1_5	[1]

Standard:

[1] RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1: https://tools.ietf.org/html/rfc3447