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 (znak s dekadickým kódem 124 v kódování Unicode podle části A přílohy k této vyhlášce). Vybranými údaji o evidované tržbě jsou v následujícím 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.

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

(4) 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 pěti skupin po osmi znacích oddělených pomlčkou (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.

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

Odůvodnění

I. Obecná část

1. Vysvětlení nezbytnosti navrhované právní úpravy, odůvodnění jejích hlavních principů

Předkládaná vyhláška je prováděcím předpisem k zákonu o evidenci tržeb. Zmocnění k vydání této vyhlášky je dáno samotným zákonem v jeho ustanovení § 19 odst. 3, které zmocňuje Ministerstvo financí ke stanovení způsobu tvorby bezpečnostního kódu poplatníka a způsobu tvorby podpisového kódu poplatníka.

Součástí komplexního řešení evidence tržeb, jehož vybrané aspekty je nutné promítnout do znění legislativní úpravy, jsou zvláštní kryptografické parametry systému. Jejich účelem je zejména zajistit, aby každá transakce, která je systémem evidence tržeb evidována, byla unikátním způsobem identifikována tak, aby nebyla možná její záměna s jinou transakcí. Prvek této individualizace transakce v sobě nese jak datová zpráva zasílaná poplatníkem správci daně, tak vlastní účtenka.

Návrh zákona o evidenci tržeb předpokládá mimo jiné tři unikátní identifikátory účtenky, a to

- **fiskální identifikační kód**, který představuje unikátní identifikátor účtenky v systémech správce daně; je generován správcem daně dle jeho vlastního klíče, tj. není třeba ho normovat formou vyhlášky,
- **podpisový kód poplatníka**, odvozený z údajů na účtence, který je generován poplatníkem vždy, na účtenku je však povinně uváděn pouze v případech, kdy na účtenku nelze uvést fiskální identifikační kód.
- **bezpečnostní kód poplatníka**, odvozený z podpisového kódu poplatníka, který je generován poplatníkem vždy a je i vždy uváděn na účtence,

S ohledem na nezbytnost zabezpečení celého systému musí mechanismus tvorby fiskálního identifikačního kódu podléhat zabezpečení a bude neveřejný.

Normovat postup tvorby je tedy třeba pouze pro bezpečnostní kód poplatníka a podpisový kód poplatníka, které jsou vytvářeny poplatníkem.

Účelem bezpečnostního kódu poplatníka je jednoznačná provazba mezi poplatníkem a jím vydanou účtenkou, přičemž dosažení tohoto účelu je sledováno stanovením specifického technického postupu tvorby tohoto datového údaje (výstupu) na zařízení poplatníka. Bezpečnostní kód poplatníka je součástí vybraných úkonů při evidenci tržeb (je obsažen mezi údaji zasílanými správci daně a údaji uváděnými na vystavené účtence).

Podpisový kód poplatníka se na účtenku uvádí v případech, kdy podle zákona o evidenci tržeb není poplatník povinen uvádět fiskální identifikační kód. Jeho cílem je zachování dvojice ochranných prvků účtenky. I pro tvorbu podpisového kódu poplatníka je stanoven zvláštní postup.

Definování postupu tvorby těchto bezpečnostních prvků je nutnou součástí legislativního řešení již v okamžiku spuštění systému evidence tržeb. Jedná se o ryze technickou vyhlášku, která v sobě obsahuje v principu toliko konkretizaci standardu tvorby a zabezpečení jednoznačnosti zmíněných identifikátorů nezbytných pro řádné fungování celého sytému evidence tržeb.

Předmět úpravy této vyhlášky úzce souvisí s technickou specifikací (upravující mj. formát a strukturu zasílaných údajů o evidované tržbě) zveřejněnou správcem daně podle § 18 odst. 4 zákona o evidenci tržeb.[1]

2. Zhodnocení souladu navrhované právní úpravy se zákonem, k jehož provedení je navržena, a s předpisy Evropské unie, judikaturou soudních orgánů Evropské unie a obecnými právními zásadami práva Evropské unie

Navrhovaná právní úprava navazuje na zákonné zmocnění vyplývající z § 19 odst. 3 zákona o evidenci tržeb, podle kterého Ministerstvo financí stanoví vyhláškou způsob tvorby bezpečnostního kódu poplatníka a podpisového kódu poplatníka.

Oprávnění Ministerstva financí vydávat v mezích své působnosti vyhlášky vyplývá z čl. 79 odst. 3 Ústavy České republiky, podle kterého ministerstva, jiné správní úřady a orgány územní samosprávy mohou na základě a v mezích zákona vydávat právní předpisy, jsou-li k tomu zákonem zmocněny. Zároveň je třeba dbát ustanovení čl. 11 odst. 5 Listiny základních práv a svobod, podle kterého lze daně a poplatky ukládat jen na základě zákona, a čl. 4 odst. 1 Listiny základních práv a svobod, podle něhož mohou být povinnosti ukládány toliko na základě zákona a v jeho mezích.

Prováděcím právním předpisem, tedy vyhláškou, dle ustálené judikatury Ústavního soudu mohou být v souladu s výše uvedenou ústavní podmínkou jednotlivcům ukládány povinnosti, ovšem nikoliv povinnosti primární, tedy tyto základní povinnosti musí být stanoveny alespoň rámcově, ale přitom dostatečně jasně a určitě právním předpisem o síle zákona, který potom podzákonný právní předpis pouze upřesňuje.

Zmocnění k vydání prováděcího právního předpisu musí přitom dostatečně jasně a určitě definovat otázky, jež zákonodárce přenechává právní úpravě v podzákonném předpisu, a zároveň nesmí tento prostor vymezovat natolik široce, aby prováděcí předpis zasahoval do sféry vyhrazené právnímu předpisu o síle zákona, tedy především právě do úpravy primárních povinností.

Zákon o evidenci tržeb upravuje dostatečně jasně a určitě základní rámec práv a povinností, jejichž specifikace je obsažena v předkládaném návrhu vyhlášky.

Ponechání vymezení uvedených aspektů evidence na úpravě prováděcí vyhlášky je odůvodnitelné zejména detailní a technickou povahou obou identifikátorů.

Vyhláška je v plném souladu se zmocněním daným zákonem o evidenci tržeb.

Oblast vyhlášky není upravena sekundárním právem Evropské unie a obecně nepodléhá harmonizaci na úrovni Evropské unie. V této oblasti má Rada pouze pravomoc přijímat směrnice ke sbližování vnitrostátních právních předpisů, které mají přímý vliv na vytváření nebo fungování vnitřního trhu, a to na základě čl. 115 Smlouvy o fungování Evropské unie (dále jen „SFEU“). Kromě toho jsou členské státy povinny při výkonu svých pravomocí respektovat principy dané SFEU (zejména články 18, 45, 49, 56, 63) a dbát na to, aby nedocházelo k neodůvodněné diskriminaci na základě státní příslušnosti nebo neodůvodněnému omezování volného pohybu osob, služeb a kapitálu nebo svobody usazování, jak bylo opakovaně potvrzeno Soudním dvorem Evropské unie. Navrhovaná právní úprava není s těmito principy v rozporu.

Navrhovaná právní úprava je tedy plně slučitelná s předpisy Evropské unie, judikaturou soudních orgánů Evropské unie a obecnými právními zásadami práva Evropské unie.

[1] viz http://www.e-trzby.cz/cs/527

3. Předpokládaný hospodářský a finanční dosah navrhované právní úpravy, sociální dopady a dopady na životní prostředí

Pokud jde o předpokládaný hospodářský a finanční dosah navrhované právní úpravy, lze odkázat na důvodovou zprávu k zákonu o evidenci tržeb, k jehož provedení je tato vyhláška navrhována. Sama o sobě však vyhláška žádný hospodářský a finanční dosah nemá, neboť toliko stanovuje tvorbu příslušných identifikátorů transakce.

Navrhovaná právní úprava nemá tedy přímý vliv na podnikatelské prostředí, na ostatní veřejné rozpočty, na specifické skupiny obyvatel včetně národnostních menšin ani na životní prostředí.

4. Zhodnocení současného stavu a dopadů navrhovaného řešení ve vztahu k zákazu diskriminace

Současná právní úprava ani navrhovaná právní úprava nemá dopad ve vztahu k zákazu diskriminace.

5. Zhodnocení dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů

Hlavním cílem návrhu vyhlášky je provedení vybraných aspektů evidence tržeb stanovením způsobu tvorby bezpečnostního kódu poplatníka a způsobu tvorby podpisového kódu poplatníka. U vyhlášky k provedení zákona o evidenci tržeb ani u tohoto zákona se nepředpokládá dopad na ochranu soukromí a na ochranu osobních údajů.

6. Zhodnocení korupčních rizik navrhovaného řešení (CIA)

Navrhovaná právní úprava není z korupčního hlediska riziková, neboť upravuje pouze technické řešení tvorby podpisového kódu poplatníka a bezpečnostního kódu poplatníka. Nemá tedy dopad na postavení konkrétních osob a nezavádí diskreci v rozhodování, v níž by mohla být korupční rizika spatřována.

7. Závěrečná zpráva z hodnocení dopadů regulace (RIA)

K zákonu o evidenci tržeb, k jehož provedení je tato vyhláška navrhována, byla zpracována podrobná závěrečná zpráva z hodnocení dopadů regulace (RIA), která je součástí důvodové zprávy, a je možno na ni odkázat pro hodnocení dopadů právní úpravy navrhované v této vyhlášce.

II. Zvláštní část

K § 1:

Stanoví se závazný technický postup tvorby podpisového kódu poplatníka, který je poplatník povinen uvádět při stanovených úkonech podle zákona o evidenci tržeb.

Podpisový kód poplatníka je ochranným prvkem, který umožňuje kontrolu integrity účtenky (tedy skutečnosti, že data, která správce daně obdržel od poplatníka, jsou správná a úplná) a prokazuje vazbu mezi poplatníkem a účtenkou (tedy zejména to, že data nevytvořil nikdo jiný než poplatník nebo je nikdo jiný nepozměnil). Vzhledem k využití soukromého kryptografického klíče, kterým disponuje pouze poplatník, není nikdo jiný než poplatník schopen vygenerovat podpisový kód poplatníka.

Kód je určen pro specifické potřeby kontroly (kontrolních orgánů/pracovníků) a není využíván zákazníkem. Délka podpisového kódu poplatníka je 344 znaků.

Podpisový kód poplatníka je vždy přenášen elektronicky do centrálního IT systému evidence tržeb a je povinně uváděn na účtence v případech překročení mezní doby odezvy (tzv. off-line režimu) nebo v případě zjednodušeného režimu, tzn. ve všech případech, kdy účtenka neobsahuje fiskální identifikační kód, protože tento kód účtence v okamžik tisku nebyl ještě správcem daně přiřazen.

Podpisový kód poplatníka se generuje z vybraných údajů o evidované tržbě zasílaných poplatníkem datovou zprávou, tj. z daňového identifikačního čísla poplatníka, který tržbu eviduje, označení provozovny, označení pokladního zařízení, pořadového čísla účtenky, data a času přijetí tržby a celkové částky tržby (na dvě desetinná místa). Z popsaných údajů se v tomto pořadí vytvoří tzv. řetězec údajů o evidované tržbě, kdy jednotlivé údaje jsou odděleny svislým oddělovačem („|“) a uvedeny ve stejné struktuře, ve které jsou zasílány datovou zprávou. Struktura těchto údajů je popsána v technické specifikaci zveřejněné správcem daně podle § 18 odst. 4 zákona o evidenci tržeb.[2]

V konkrétním případě může textový řetězec údajů vypadat takto: „CZ72080043|181|00/2535/CN58|0/2482/IE25|2016-12-07T22:01:00+01:00|87988.00“.

V uvedeném příkladu jde o údaje o účtence, kterou vydal poplatník s DIČ CZ72080043 v provozovně č. 181 na pokladním zařízení označeném jako „00/2535/CN58“. Účtenka byla vydána s pořadovým číslem „0/2482/IE25“, k jejímu vydání došlo 7. prosince 2016 ve 22:01 středoevropského času a částka tržby činila 87 988 Kč.

Z tohoto řetězce je následně za pomoci kryptografické hashovací funkce SHA-256 vytvořen tzv. otisk (hash), který je poté podepsán podpisovým schématem RSASSA-PKCS1-v1_5 platným soukromým klíčem k používanému certifikátu pro evidenci tržeb. Takto podepsaný otisk řetězce údajů o evidované tržbě vyjádřený v kódování Base64 tvoří podpisový kód poplatníka.

Kryptografické hashovací funkce jsou konstruovány takovým způsobem, aby při dvou shodných vstupech vygenerovaly dva shodné otisky. Při dvou (byť jen nepatrně) rozdílných vstupech naopak s vysokou pravděpodobností vygenerují otisky různé.

Asymetrická šifrovací metoda RSA je matematickou metodou založenou na dvou šifrovacích klíčích S (soukromý) a V (veřejný), pro které platí, že zprávu zašifrovanou klíčem S lze rozšifrovat pouze klíčem V a naopak zprávu zašifrovanou klíčem V lze rozšifrovat pouze

[2] viz http://www.e-trzby.cz/cs/527

klíčem S. Klíč S má k dispozici pouze poplatník a uchovává jej v tajnosti, zatímco klíč V je na rozdíl od toho veřejně dostupný, a má jej tedy k dispozici i správce daně. Tuto šifrovací metodu je možno využít buď k šifrování zpráv (zprávu odesílatel zašifruje klíčem V a rozšifrovat ji bude moct pouze osoba disponující klíčem S), nebo k podepisování zpráv. Spolu se zprávou se pošle i její podpis, který tvoří tato zpráva zašifrovaná pomocí klíče S. Příjemce zprávy tento podpis rozšifruje klíčem V a výsledek porovná se zaslanou zprávou. Pokud se přijatá zpráva a podpis rozšifrovaný klíčem V shodují, lze konstatovat, že podpis byl vytvořen pomocí klíče S (který je párový ke klíči V). Klíč S je ale udržován v tajnosti a má ho k dispozici pouze osoba, která vydala klíč V použitý k ověření podpisu. Lze tedy učinit závěr, že zprávu podepsala právě tato osoba. Podpisové schéma RSASSA-PKCS1-v1_5 je pak konkrétním technickým standardem, který konkretizuje popsanou matematickou metodu pro její praktické využití.

Nevýhodou techniky podepisování popsané v předchozím odstavci, která využívá bez dalšího samotné podpisové schéma založené na asymetrické šifrovací metodě RSA, je její relativně vyšší výpočetní náročnost. Druhou nevýhodou je délka podpisu, protože podpis je stejně dlouhý jako samotná podepisovaná zpráva. Z toho důvodu se v praxi využívá kombinace podpisového schématu s výše popsanými kryptografickými hashovacími funkcemi. Pomocí hashovací funkce se zkonstruuje otisk zprávy a soukromým klíčem S se zašifruje tento otisk. Při ověřování podpisu se porovnává otisk získaný rozšifrováním podpisu s otiskem, který ověřovatel zkonstruuje z doručené zprávy. Na tomto principu fungují elektronické podpisy využívané v praxi (například při podpisu emailových zpráv).

Data jsou v paměti počítače standardně uchovávána v tzv. osmibitovém kódování, tedy jako číslice v rozsahu 0 až 255 (což je 256 neboli 2^8 číslic). Počítač pak jednotlivým číslicím přiřazuje pomocí kódovacích tabulek konkrétní znaky (například číslice 65 v kódovací tabulce ASCII odpovídá znaku „A“). Některé znaky v osmibitovém kódování však nelze bez dalšího vložit do souboru ve struktuře XML, ve které budou odesílány údaje o účtence. Z toho důvodu se standardně pro reprezentaci dat používá tzv. kódování Base64, které používá číslice v rozsahu 0 až 63 (tedy 64 číslic) a přiřazuje jim znaky, které nejsou v rozporu s formátem XML.

Při ověřování integrity zaslaných dat a jejich vazby na konkrétního poplatníka nejprve správce daně rozšifruje zaslaný podpisový kód poplatníka, čímž získá otisk řetězce údajů o evidované tržbě za pomoci veřejného klíče tohoto poplatníka. Tento otisk pocházející z podpisového kódu poplatníka následně porovná s otiskem, který si správce daně sám vytvoří z vybraných údajů o evidované tržbě zaslaných poplatníkem datovou zprávou. Pokud se otisky získané rozšifrováním podpisového kódu poplatníka a získané přímo výpočtem z dat shodují, pak lze s vysokou mírou pravděpodobnosti tvrdit, že s údaji nebylo manipulováno a že je správci daně zaslal právě tento poplatník a nikdo jiný.

K § 2:

Stanoví se závazný technický postup tvorby bezpečnostního kódu poplatníka, který je poplatník povinen uvádět při stanovených úkonech podle zákona o evidenci tržeb.

Zatímco podpisový kód poplatníka slouží k ochraně integrity údajů o účtence a k potvrzení vztahu těchto dat a konkrétního poplatníka, bezpečnostní kód poplatníka slouží k ochraně integrity samotného podpisového kódu poplatníka. Jde tedy o druhou úroveň ochrany přenášených dat. Tento kód je vždy přenášen elektronicky do centrálního IT systému evidence tržeb a uváděn na účtence.

Bezpečnostní kód poplatníka se generuje z podpisového kódu poplatníka, kdy se nejprve podpisový kód poplatníka převede z kódování Base 64 do osmibitového kódování a následně

se z něj vytvoří otisk za pomoci kryptografické hashovací funkce SHA-1. Tento otisk podpisového kódu poplatníka se vyjádří v kódování Base16 a uvede ve formě pěti skupin po osmi znacích oddělených pomlčkou. Kódování Base16 používá číslice v rozsahu 0 až 15 (tedy 16 číslic) a přiřazuje jim znaky 0 až 9 a A až F. Délka bezpečnostního kódu poplatníka je 40 znaků bez oddělovacích znaků (pomlčky).

Z popsaných vlastností kryptografických hashovacích funkcí plyne, že pro různé podpisové kódy poplatníka (a tedy obsahem různé účtenky) budou odpovídající bezpečnostní kódy poplatníka také různé.

Bezpečnostní kód poplatníka tak má vlastnosti unikátního identifikátoru účtenky se silnou vazbou na jejího vystavitele a její obsah. Každou účtenku bude možné pomocí bezpečnostního kódu poplatníka ztotožnit s údaji v systémech evidence tržeb, což může být využito jak správcem daně při kontrole, zda je daný exemplář účtenky evidován, tak lze tento kód využít jako identifikátor výherní účtenky v účtenkové loterii.

Bezpečnostní kód poplatníka (spolu s podpisovým kódem) slouží zároveň k ochraně daného poplatníka před rizikem falšování účtenek jinou osobou jeho jménem. Vzhledem k využití údajů známých pouze poplatníkovi (soukromý kryptografický klíč) není nikdo jiný než poplatník schopen vygenerovat podpisový kód poplatníka a následně ani bezpečnostní kód poplatníka, který by uvedl na výtisk účtenky.

K § 3:

Stanoví se okamžik nabytí účinnosti této vyhlášky, a to 1. prosince 2016.

K příloze k vyhlášce:

V příloze jsou specifikovány standardy kódování, kryptografických hashovacích funkcí a podpisového schématu, a to včetně odkazů na tyto standardy.