

## 194/2009 Sb.

### VYHLÁŠKA

ze dne 23. června 2009

#### **o stanovení podrobností užívání a provozování informačního systému datových schránek**

Změna: 422/2010 Sb.  
Změna: 322/2015 Sb.  
Změna: 435/2016 Sb.  
Změna: 216/2018 Sb.  
Změna: 216/2018 Sb. (část)  
Změna: 318/2023 Sb.

Ministerstvo vnitra stanoví podle § 9 odst. 3 a 4, § 20 odst. 3 a § 21 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění zákona č. 190/2009 Sb.:

#### § 1

##### **Náležitosti přístupových údajů pro přihlašování do datové schránky**

- (1) Přístupové údaje pro přihlašování do datové schránky tvoří uživatelské jméno a bezpečnostní heslo.
- (2) Uživatelské jméno je pro každou osobu jedinečné.
- (3) Uživatelské jméno je řetězec nejméně 6 a nejvýše 12 znaků vzniklý automatizovaným generováním.
- (4) Přípustné znaky pro tvorbu uživatelského jména a bezpečnostního hesla jsou uvedeny v příloze č. 1 k této vyhlášce.
- (5) Bezpečnostní heslo
  - a) nesmí být shodné s uživatelským jménem, se kterým tvoří jedny přístupové údaje,
  - b) musí obsahovat nejméně 8 znaků a nejvýše 64 znaků,
  - c) musí obsahovat alespoň jedno velké písmeno, jedno malé písmeno a jednu číslici,
  - d) nesmí obsahovat 3 a více shodných znaků opakujících se za sebou,
  - e) nesmí začínat textem "qwert", "asdfg" nebo "12345" a
  - f) nesmí být shodné s naposledy použitými 255 bezpečnostními hesly.

#### § 2

##### **Elektronické prostředky pro přihlašování do datové schránky**

- (1) Pro přihlašování do datové schránky lze použít elektronický prostředek, který je kryptografickým prostředkem
  - a) obsahujícím soukromý kryptografický klíč a veřejný kryptografický klíč, které jsou vytvořeny a užívány s využitím některého z algoritmů uvedených v bodu I přílohy č. 2 k této vyhlášce,
  - b) obsahujícím certifikát sloužící k autentizaci uživatele (dále jen „autentizační certifikát“), který je vytvořen a užíván s využitím hashovací funkce uvedené v bodu II přílohy č. 2 k této vyhlášce a s využitím algoritmů podle písmene a),
  - c) umožňujícím vytvoření, uložení a použití soukromého kryptografického klíče a veřejného kryptografického klíče a autentizačního certifikátu ve formátu stanoveném v souladu se standardem uvedeným v bodu III písm. a) přílohy č. 2 k této vyhlášce; autentizační certifikát obsahuje
    1. údaje umožňující identifikovat osobu, která se přihlašuje do informačního systému datových schránek,
    2. obchodní firmu nebo název kvalifikovaného poskytovatele služeb vytvářejících důvěru, 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 kvalifikovaný poskytovatel služeb vytvářejících důvěru usazen,
    3. číslo autentizačního certifikátu unikátní u daného kvalifikovaného poskytovatele služeb vytvářejících důvěru a
    4. údaje o počátku a konci platnosti autentizačního certifikátu,
  - d) neumožňujícím přenos soukromého kryptografického klíče podle písmene a) z tohoto elektronického prostředku,
  - e) podporujícím použití některého z algoritmů uvedených v bodu I přílohy č. 2 k této vyhlášce a hashovací funkce uvedené v bodu II přílohy č. 2 k této vyhlášce,

f) jehož použití je podmíněno zadáním bezpečnostního kódu (PIN) a

g) u něhož není známo zvýšené riziko ohrožující provoz informačního systému datových schránek.

(2) Autentizační certifikát podle odstavce 1 písm. b) vydává kvalifikovaný poskytovatel služeb vytvářejících důvěru.

(3) Pro přihlašování do datové schránky lze dále použít elektronický prostředek, který je spojením mobilního zařízení a mobilní aplikace poskytované Ministerstvem vnitra. Takový elektronický prostředek musí splňovat technické specifikace a postupy stanovené pro vlastnosti a formu prostředků pro elektronickou identifikaci, autentizaci a technické kontroly přímo použitelným předpisem Evropské unie upravujícím minimální technické specifikace a postupy pro úroveň záruky prostředků pro elektronickou identifikaci<sup>1)</sup>, a to alespoň pro značnou úroveň záruky.

### § 3

#### **Technické podmínky a bezpečnostní zásady pro přístup do datové schránky**

(1) Přihlašuje-li se osoba oprávněná k přístupu do datové schránky prostřednictvím elektronického prostředku podle § 2 odst. 1, správce informačního systému datových schránek neumožní přihlášení bez současného zadání uživatelského jména a bezpečnostního hesla podle § 1. Užívá-li osoba oprávněná k přístupu do datové schránky k přihlašování elektronický prostředek podle § 2 odst. 1, správce informačního systému datových schránek této osobě neumožní přihlášení pouze přístupovými údaji podle § 1.

(2) Je-li při přihlašování do datové schránky prostřednictvím přístupových údajů podle § 1 bezprostředně po sobě po páté chybně zadáno bezpečnostní heslo, správce informačního systému datových schránek je oprávněn znemožnit přihlášení do datové schránky prostřednictvím stejného uživatelského jména po dobu až 1 hodiny od okamžiku pátého chybného zadání bezpečnostního hesla. Správce informačního systému datových schránek současně zašle na elektronickou adresu zvolenou osobou, pro niž byla datová schránka zřízena, nebo administrátorem, sdělení, že došlo k pokusu o neoprávněné přihlášení do datové schránky a že se osobě oprávněné k přístupu do datové schránky doporučuje, aby bez prodlení provedla změnu bezpečnostního hesla. Věta první a druhá se nepoužije, přihlašuje-li se osoba oprávněná k přístupu do datové schránky prostřednictvím elektronických prostředků podle § 2.

(3) Neprovede-li osoba oprávněná k přístupu do datové schránky, která je do datové schránky přihlášená, v datové schránce žádný úkon po dobu 30 minut, správce informačního systému datových schránek tuto osobu z datové schránky odhlásí. Věta první se nepoužije, je-li do datové schránky přístupováno prostřednictvím elektronického systému spisové služby nebo jiné elektronické aplikace s užitím certifikátu.

(4) Správce informačního systému datových schránek umožní osobě oprávněné k přístupu do datové schránky kdykoliv změnit bezpečnostní heslo. Změnu bezpečnostního hesla lze provést způsobem umožňujícím dálkový přístup.

(5) Přihlášení do datové schránky prostřednictvím elektronického prostředku podle § 2 odst. 1 se řídí bezpečnostními zásadami uvedenými v certifikační politice, kterou kvalifikovaný poskytovatel služeb vytvářejících důvěru vede v souladu s technickými normami uvedenými v bodu III písm. b) a c) přílohy č. 2 k této vyhlášce a zveřejňuje ji způsobem umožňujícím dálkový přístup.

### § 4

#### **Přípustné formáty datové zprávy dodávané do datové schránky**

Přípustné formáty datové zprávy dodávané do datové schránky jsou stanoveny v příloze č. 3 k této vyhlášce.

### § 5

#### **Maximální velikost datové zprávy dodávané do datové schránky**

Maximální velikost datové zprávy dodávané do datové schránky činí 100 MB.

### § 6

#### **Doba uložení datové zprávy v datové schránce**

Doba uložení datové zprávy v datové schránce činí

a) 90 dnů ode dne, kdy se do datové schránky přihlásila osoba, která má s ohledem na rozsah svého oprávnění k dokumentu obsaženému v datové zprávě přístup,

b) 90 dnů ode dne, kdy bylo do datové schránky přistoupeno prostřednictvím elektronického systému spisové služby nebo jiné elektronické aplikace s užitím certifikátu,

c) 3 roky ode dne, kdy byla datová zpráva dodána do datové schránky, nedojde-li k přístupu do datové schránky podle písmene a) nebo b).

### § 7

#### **Technické náležitosti užívání datové schránky**

Správce informačního systému datových schránek nepřijme k odeslání datovou zprávu,

a) není-li v přípustném formátu stanoveném touto vyhláškou,

b) převyšuje-li její velikost maximální velikost stanovenou touto vyhláškou, nebo

c) vyžaduje-li to plnění povinnosti zajistit dostupnost, důvěrnost a integritu informačního systému datových schránek nebo jiného informačního systému a informací v nich obsažených.

## § 8

### Způsob tvorby identifikátoru datové schránky

(1) Správce informačního systému datových schránek vytváří identifikátor datové schránky automatizovaně s využitím algoritmů pro generování náhodných čísel.

(2) Identifikátor datové schránky je pro každou datovou schránku jedinečný.

## § 9

### Účinnost

Tato vyhláška nabývá účinnosti dnem 1. července 2009.

Ministr:

**Ing. Pecina, MBA v. r.**

### Příloha 1

#### Přípustné znaky pro tvorbu uživatelského jména a bezpečnostního hesla

##### I. Písmena a číslice

-----  
Přípustný ASCII kód  
znak           přípustného  
                  znaku  
-----

0	48
1	49
2	50
3	51
4	52
5	53
6	54
7	55
8	56
9	57
A	65
B	66
C	67
D	68
E	69
F	70
G	71
H	72
I	73
J	74
K	75
L	76
M	77
N	78
O	79
P	80
Q	81
R	82
S	83
T	84
U	85
V	86
W	87
X	88
Y	89

Z	90
a	97
b	98
c	99
d	100
e	101
f	102
g	103
h	104
i	105
j	106
k	107
l	108
m	109
n	110
o	111
p	112
q	113
r	114
s	115
t	116
u	117
v	118
w	119
x	120
y	121
z	122

-----

## II. Speciální znaky

-----

Přípustný ASCII kód	
znak	přípustného
	znaku

-----

(mezera)	32
!	33
#	35
\$	36
%	37
&	38
(	40
)	41
*	42
+	43
,	44
-	45
.	46
:	58
=	61
?	63
@	64
[	91
]	93
_	95
{	123
	124
}	125
~	126

-----

## Příloha 2

### Seznam algoritmů, hashovacích funkcí, standardů a technických norem

#### I. Algoritmy

- a) RSA 2048 a 3072 bitů (RFC 8017)
- 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 180-4)

## III. Standard a technické normy

a) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

b) ETSI EN 319 401 v2.1.1 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

c) ETSI EN 319 411-1 v1.1.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

## Příloha 3

### Přípustné formáty datové zprávy dodávané do datové schránky

I. Přípustnými formáty datové zprávy dodávané do datové schránky jsou za splnění podmínky uvedené v bodu IV formáty

a) pdf (Portable Document Format),

b) PDF/A (Portable Document Format for the Long-term Archiving),

c) xml (Extensible Markup Language Document)\*,

d) fo/zfo (602XML Filler dokument),

e) html/htm (Hypertext Markup Language Document),

f) odt (Open Document Text),

g) ods (Open Document Spreadsheet),

h) odp (Open Document Presentation),

i) txt/csv (prostý text),

j) rtf (Rich Text Format),

k) doc/docx (MS Word Document),

l) xls/xlsx (MS Excel Spreadsheet),

m) ppt/pptx (MS PowerPoint Presentation),

n) jpg/jpeg/jfif (Joint Photographic Experts Group File Interchange Format),

o) png (Portable Network Graphics),

p) tif/tiff (Tagged Image File Format),

q) gif (Graphics Interchange Format),

r) mpg/mpeg/mpeg1/mpeg2 (MPEG Phase 1 -ISO-IEC 11172/Phase 2 - ISO//ISO/IEC 13818),

s) wav (Waveform Audio Format),

t) mp2/mp3 (MPEG-1 Audio Layer 2/Layer 3),

u) isdoc/isdocx (Information System Document) verze 5.2 a vyšší,

v) edi (mezinárodní standard EDIFACT, standardy ODETTE a EANCOM pro elektronickou výměnu obchodních dokumentů - EDI),

w) dwg (AutoCAD DraWinG File Format) verze 2007 a vyšší,

x) shp/dbf/shx/prj/qix/sbn/sbx (ESRI Shapefile),

y) dgn (Bentley MicroStation Format) verze V7 a V8 a

z) gml/gfs/xsd (Geography Markup Language Document).

**II.** Přípustnými formáty datové zprávy dodávané do datové schránky jsou za splnění podmínky uvedené v bodu IV formáty.

- a) json (JavaScript Object Notation),
- b) mp4/m4a (MPEG-4 Audio ISO/IEC 14496),
- c) mp4/m4v/m4p (MPEG-4 Video ISO/IEC 14496) a
- d) heic/heif (High Efficiency Image File).

**III.** Přípustnými formáty datové zprávy dodávané do datové schránky jsou za splnění podmínek uvedených v bodech IV až VI formáty.

- a) zip (ZIP File Format, specifikovaný v Info-ZIP Application Note 19970311) a
- b) asics/scs/asice/sce (Associated Signature Containers Simple / Extended).

**IV.** Formáty uvedené v bodech I až III jsou přípustnými formáty datové zprávy dodávané do datové schránky, obsahuje-li název souboru tvořící datovou zprávu jím odpovídající příponu. Příponou se rozumí vnější znak formátu datové zprávy, který umožňuje programovému vybavení určení typu datového souboru.

**V.** Formáty uvedené v bodu III jsou přípustnými formáty datové zprávy dodávané do datové schránky, pokud

- a) obsah datové zprávy není zašifrovaný,
- b) datovou zprávu tvoří alespoň jeden soubor ve formátu uvedeném v bodu I nebo II,
- c) datovou zprávu tvoří soubor v jiném formátu než ve formátu uvedeném v bodu I nebo II,
- d) datovou zprávu tvoří nejvýše 1 000 souborů a adresářů,
- e) maximální úroveň vnoření adresářů do sebe činí 4 a
- f) maximální velikost dekomprimovaného obsahu činí 3 GB.

**VI.** Formát uvedený v bodu III písm. a) je přípustným datovým formátem datové zprávy dodávané do datové schránky, pokud datovou zprávu tvoří soubor obsahující část komprimovaného obsahu.

---

1) Prováděcí nařízení Komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úroveň záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu.