VYHLÁŠKA

ze dne 23. června 2009

o stanovení podrobností užívání a provozování informačního systému datových schránek

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. …/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) Bezpečnostní heslo je řetězec nejméně 8 a nejvýše 32 znaků. Vždy se jedná o kombinaci písmen, číslic a speciálních znaků.

(5) Přípustné znaky pro tvorbu uživatelského jména a bezpečnostního hesla jsou uvedeny v příloze č. 1 k této vyhlášce.

(6) Bezpečnostní heslo nesmí být shodné s uživatelským jménem, se kterým tvoří přístupové údaje.

§ 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 některé z hashovacích funkcí uvedených 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 podle technické normy uvedené 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 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 poskytovatel certifikačních služeb usazen,

3. číslo autentizačního certifikátu unikátní u daného poskytovatele certifikačních služeb 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 některé z hashovacích funkcí uvedených 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 akreditovaný poskytovatel certifikačních služeb.

§ 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, 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, 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 neumožní přihlášení do datové schránky prostřednictvím stejného uživatelského jména po dobu 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 elektronického prostředku podle § 2.

(3) Neprovede-li osoba oprávněná k přístupu do datové schránky, která je do datové schránky přihlášena, 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 přistupováno prostřednictvím elektronického systému spisové služby nebo jiné elektronické aplikace s užitím systémového 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 se řídí bezpečnostními zásadami uvedenými v certifikační politice, kterou poskytovatel

certifikačních služeb vede v souladu se standardem uvedeným v bodu III písm. b) 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 10 MB.

§ 6

Doba uložení datové zprávy v datové schránce

(1) Doba uložení datové zprávy v datové schránce činí 90 dnů ode dne, kdy se do této datové schránky přihlásila osoba, která má s ohledem na rozsah svého oprávnění k dokumentu obsaženému v datové zprávě přístup. Byla-li datová zpráva do datové schránky dodána způsobem podle § 18a zákona o elektronických úkonech a autorizované konverzi dokumentů, doba uložení datové zprávy v datové schránce činí 90 dnů ode dne dodání.

(2) Je-li do datové schránky přistupováno prostřednictvím elektronického systému spisové služby nebo jiné elektronické aplikace s užitím systémového certifikátu, doba uložení datové zprávy v datové schránce činí 90 dnů ode dne, kdy bylo do této datové schránky přistoupeno prostřednictvím elektronického systému spisové služby nebo jiné elektronické aplikace s užitím systémového certifikátu.

§ 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) obsahuje-li škodlivý kód, který může poškodit informační systém datových schránek, údaj v něm obsažený nebo výpočetní techniku držitele datové schránky.

§ 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

Příloha č. 1 k vyhlášce č. …/2009 Sb.

Přípustné znaky pro tvorbu uživatelského jména a bezpečnostního hesla

I. Písmena a číslice

Přípustný znak	ASCII kód 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

Přípustný znak	ASCII kód přípustného znaku
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

Přípustný znak	ASCII kód přípustného znaku
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 znak	ASCII kód přípustného znaku
!	33
#	35
$	36
%	37
&	38
(	40
)	41
*	42

Přípustný znak	ASCII kód přípustného znaku
+	43
,	44
-	45
.	46
:	58
=	61
?	63
@	64

Přípustný znak	ASCII kód přípustného znaku
[	91
]	93
_	95
{	123
|	124
}	125
~	126

Příloha č. 2 k vyhlášce č. …/2009 Sb.

Seznam algoritmů, hashovacích funkcí, standardů a technických norem

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

a) SHA-1 (FIPS 180-2)

b) SHA-2 – 256, 384, 512 bitů (FIPS 180-2)

c) RIPEMD-160

III. Standardy a technické normy

a) ČSN ISO/IEC 9594-8 Informační technologie – Propojení otevřených systémů – Adresář: Základní struktury certifikátu veřejného klíče a certifikátu atributu

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

Příloha č. 3 k vyhlášce č. …/2009 Sb.

Přípustné formáty datové zprávy dodávané do datové schránky

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 (prostý text)

j) rtf (Rich Text Format)

k) doc (MS Word Document)

l) xls (MS Excel Spreadsheet)

m) ppt (MS PowerPoint Presentation)

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

o) png (Portable Network Graphics)

p) tiff (Tagged Image File Format)

q) gif (Graphics Interchange Format)

r) mpeg1/mpeg2 (Moving Picture Experts Group Phase 1/Phase 2)

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

* **Pozn.** Pokud odpovídají veřejně dostupnému XSD schématu publikovanému příjemcem datové zprávy.