212

VYHLÁŠKA

ze dne 13. června 2012

o struktuře údajů, na základě kterých je možné jednoznačně identifikovat podepisující osobu, a postupech pro ověřování platnosti zaručeného elektronického podpisu, elektronické značky, kvalifikovaného certifikátu, kvalifikovaného systémového certifikátu a kvalifikovaného časového razítka (vyhláška o ověřování platnosti zaručeného elektronického podpisu)

Ministerstvo vnitra stanoví podle § 20 odst. 4 zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění zákona č. 517/2002 Sb., zákona č. 440/2004 Sb., zákona č. 424/2010 Sb. a zákona č. 167/2012 Sb.:

§ 1

Struktura údajů, na základě kterých je možné jednoznačně identifikovat podepisující osobu

Údaj, který umožňuje jednoznačnou identifikaci podepisující osoby, se uvádí ve struktuře desetimístného čísla v desítkové soustavě v rozsahu 1 100 100 100 až 4 294 967 295.

§ 2

Ověření platnosti zaručeného elektronického podpisu nebo elektronické značky

Platnost zaručeného elektronického podpisu, kterým je podepsána datová zpráva, nebo elektronické značky, kterou je označena datová zpráva, se ověřuje podle standardu kryptografického asymetrického algoritmu uvedeného v příloze č. 1 k této vyhlášce a standardu kryptografické hashovací funkce uvedeného v příloze č. 2 k této vyhlášce, které odpovídají schématu použitému při vytváření zaručeného elektronického podpisu nebo elektronické značky.

Ověření platnosti kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu

§ 3

(1) Okamžikem, ke kterému je ověřována platnost kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu, je okamžik doručení datové zprávy, případně nejčasnější časový okamžik, ve kterém již prokazatelně existoval zaručený elektronický podpis nebo elektronická značka založené na certifikátu, jehož platnost je ověřována.

(2) Není-li kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát v okamžiku podle odstavce 1 platný, a je-li k datové zprávě podepsané elektronickým podpisem nebo označené elektronickou značkou připojeno platné kvalifikované časové razítko, ověřuje se platnost kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu k časovému údaji uvedenému v kvalifikovaném časovém razítku.

(3) Okamžikem, ke kterému je ověřována platnost kvalifikovaného systémového certifikátu, na kterém je založena elektronická značka označující kvalifikované časové razítko, je okamžik doručení datové zprávy, případně nejčasnější časový okamžik, ve kterém již prokazatelně existovalo kvalifikované časové razítko.

(4) Není-li kvalifikovaný systémový certifikát, na kterém je založena elektronická značka označující kvalifikované časové razítko, v okamžiku, ke kterému je ověřována jeho platnost, platný, a bylo-li k ověřovanému kvalifikovanému časovému razítku nebo k datové zprávě opatřené ověřovaným kvalifikovaným časovým razítkem následně připojeno v době platnosti tohoto kvalifikovaného systémového certifikátu další kvalifikované časové razítko označené elektronickou značkou založenou na kvalifikovaném systémovém certifikátu, který byl v okamžiku podle odstavce 3 platný, ověřuje se platnost kvalifikovaného systémového certifikátu, na kterém je založena elektronická značka označující ověřované kvalifikované časové razítko k časovému údaji uvedenému v následně připojeném kvalifikovaném časovém razítku.

(5) Je-li k ověřovanému kvalifikovanému časovému razítku nebo k datové zprávě opatřené ověřovaným kvalifikovaným časovým razítkem připojeno více dalších kvalifikovaných časových razítek, lze postupem uvedeným v odstavci 4 ověřit platnost kvalifikovaného časového razítka k časovému údaji uvedenému v kvalifikovaném časovém razítku připojeném následně po ověřovaném kvalifikovaném časovém razítku.

§ 4

(1) Ověření platnosti kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu zahrnuje

a) ověření, zda je kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát v intervalu doby platnosti,

b) ověření platnosti elektronické značky označující

kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát,

c) ověření, zda kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát nebyl zneplatněn, a ověření elektronické značky, kterou kvalifikovaný poskytovatel certifikačních služeb (dále jen „poskytovatel“) označil seznam zneplatněných certifikátů nebo informaci o stavu certifikátu, a kvalifikovaného systémového certifikátu poskytovatele,

d) ověření platnosti všech kvalifikovaných systémových certifikátů a elektronických značek označujících kvalifikované systémové certifikáty v certifikační cestě a

e) ověření, zda byl certifikát vydán jako kvalifikovaný certifikát nebo jako kvalifikovaný systémový certifikát.

(2) Ověření, zda kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát nebyl v okamžiku, ke kterému je ověřována jeho platnost, zneplatněn, se provádí v souladu s certifikační politikou poskytovatele, který certifikát vydal. Je-li k ověření užit seznam zneplatněných certifikátů, pro ověření je rozhodným seznamem poslední seznam, který byl vydán ve lhůtě 24 hodin od okamžiku, ke kterému je platnost certifikátu ověřována, případně každý následující seznam vydaný před koncem intervalu platnosti ověřovaného certifikátu. Pokud lhůta 24 hodin přesahuje interval platnosti ověřovaného certifikátu, jsou rozhodnými seznamy všechny seznamy vydané od posledního seznamu vydaného v intervalu platnosti certifikátu po poslední seznam, který byl vydán ve lhůtě 24 hodin od okamžiku, ke kterému je platnost certifikátu ověřována.

(3) Certifikační cestou se rozumí hierarchicky uspořádaná posloupnost certifikátů, která zahrnuje ověřovaný kvalifikovaný certifikát nebo ověřovaný kvalifikovaný systémový certifikát a kvalifikovaný systémový certifikát poskytovatele, na němž je založena elektronická značka ověřovaného kvalifikovaného certifikátu nebo ověřovaného kvalifikovaného systémového certifikátu, každý další kvalifikovaný systémový certifikát poskytovatele, na kterém je založena elektronická značka kvalifikovaného systémového certifikátu poskytovatele, který byl naposledy zahrnut do certifikační cesty, a končí kvalifikovaným systémovým certifikátem poskytovatele označeným elektronickou značkou, která je založena na něm samém.

(4) Ověření, zda certifikát, na kterém je založen zaručený elektronický podpis nebo elektronická značka, byl vydán jako kvalifikovaný certifikát nebo jako kvalifikovaný systémový certifikát, se provádí ověřením kvalifikovaného systémového certifikátu poskytovatele, na kterém je založena elektronická značka ověřovaného certifikátu, v evidenci vydaných kvalifikovaných systémových certifikátů, které používá poskytovatel, vedené Ministerstvem vnitra. Pokud byl certifikát vydán poskytovatelem certifikačních služeb usazeným v jiném státu, považuje se za kvalifikovaný, byl-li vydán v rámci služby vydávání kvalifikovaných certifikátů vedené v seznamu důvěryhodných certifikačních služeb jako služba, pro jejíž poskytování je poskytovatel certifikačních služeb akreditován, nebo jako služba, nad jejímž poskytováním je vykonáván dohled podle přímo použitelného předpisu Evropské unie[1]).

§ 5

Ověření platnosti kvalifikovaného časového razítka

(1) Ověření platnosti kvalifikovaného časového razítka zahrnuje

a) ověření vazby mezi datovou zprávou a připojeným kvalifikovaným časovým razítkem,

b) ověření platnosti elektronické značky označující kvalifikované časové razítko a

c) ověření platnosti kvalifikovaného systémového certifikátu, na kterém je založena elektronická značka označující kvalifikované časové razítko.

(2) Ověření vazby mezi datovou zprávou a připojeným kvalifikovaným časovým razítkem se provádí podle standardu kryptografické hashovací funkce odpovídající funkci použité při výpočtu otisku datové zprávy uvedeného v kvalifikovaném časovém razítku.

§ 6

Účinnost

Tato vyhláška nabývá účinnosti dnem 1. července 2012.

Ministr:

Kubice v. r.

[1]) Rozhodnutí Komise Evropských společenství 2009/767/ES ze dne 16. října 2009, kterým se stanovují opatření pro usnadnění užití postupů s využitím elektronických prostředků prostřednictvím „jednotných kontaktních míst“ podle směrnice Evropského parlamentu a Rady 2006/123/ES o službách na vnitřním trhu.

Příloha č. 1 k vyhlášce č. 212/2012 Sb.

Standardy kryptografických asymetrických algoritmů

Index asymetrického algoritmu	Zkrácený název kryptografického asymetrického algoritmu	Standardy
1.01	rsa	[1]
1.02	dsa	[2]
1.03	ecdsa-Fp	[2,3]
1.04	ecdsa-F2m	[2,3]
1.05	ecgdsa-Fp	[4]
1.06	ecgdsa-F2m	[4]

Standardy:

[1] ISO/IEC 14888-3: Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms.

[2] NIST: FIPS Publication 186-2: Digital Signature Standard (DSS).

[3] Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), ANSI X9.62-1998.

[4] ISO/IEC FCD 15946-2: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures.