496

VYHLÁŠKA

ze dne 29. července 2004

o elektronických podatelnách

Ministerstvo informatiky 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. 226/2002 Sb., zákona č. 517/2002 Sb. a zákona č. 440/2004 Sb., (dále jen „zákon“):

§ 1

Předmět úpravy

Tato vyhláška stanoví postupy orgánů veřejné moci uplatňované při přijímání a odesílání datových zpráv prostřednictvím elektronické podatelny a strukturu údajů kvalifikovaného certifikátu, na základě kterých je možné podepisující osobu při přijímání datových zpráv prostřednictvím elektronické podatelny jednoznačně identifikovat.

§ 2

Přijetí a doručení datové zprávy

(1) Nestanoví-li tato vyhláška jinak, je přijatá datová zpráva považována za doručenou orgánu veřejné moci, pokud je dostupná elektronické podatelně provozované podle zvláštního právního předpisu[1]).

(2) Pokud je u přijaté datové zprávy zjištěn výskyt chybného formátu nebo počítačového programu, jež jsou způsobilé přivodit škodu na informačním systému nebo na informacích zpracovávaných orgánem veřejné moci (dále jen „škodlivý kód“), může být datová zpráva uložena jen mimo elektronickou podatelnu, a to za předpokladu, že není ohrožena bezpečnost informačního systému orgánu veřejné moci ani bezpečnost zpracovávaných informací. Taková datová zpráva není dostupná elektronické podatelně.

(3) Doručená datová zpráva se ukládá do úložiště doručených datových zpráv ve tvaru, ve kterém byla přijata. Je-li k datové zprávě připojen kvalifikovaný certifikát a zaručený elektronický podpis založený na tomto certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb (dále jen „uznávaný elektronický podpis“) nebo kvalifikovaný systémový certifikát a elektronická značka založená na tomto certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb (dále jen „uznávaná elektronická značka“), ukládají se spolu se zprávou.

(4) Doručená datová zpráva se v elektronické podatelně

a) eviduje a dále se předává v souladu se zvláštními právními předpisy[2]) upravujícími evidenci doručených písemností a další nakládání s nimi s tím, že čas doručení datové zprávy je zaznamenán s přesností na sekundu, a

b) označuje identifikátorem elektronické podatelny, který má charakter podacího razítka.

(5) Doručení datové zprávy se potvrzuje odesilateli neprodleně zasláním datové zprávy v souladu s ustanovením § 3, pokud je orgán veřejné moci schopen z přijaté datové zprávy zjistit elektronickou adresu odesilatele. Součástí zprávy o potvrzení doručení je

a) uznávaný elektronický podpis oprávněného zaměstnance orgánu veřejné moci nebo uznávaná elektronická značka orgánu veřejné moci,

b) datum a čas s uvedením hodiny, minuty a sekundy, kdy byla datová zpráva doručena, a

c) charakteristika doručené datové zprávy umožňující její identifikaci.

(6) U doručené datové zprávy elektronická podatelna zjišťuje, zda

a) datová zpráva odpovídá technickým parametrům, které orgán veřejné moci zveřejnil podle zvláštního právního předpisu[1]),

b) je připojen uznávaný elektronický podpis nebo uznávaná elektronická značka, případně zda je připojeno kvalifikované časové razítko, pokud zvláštní právní předpis stanoví povinnost připojit jej k datové zprávě,

c) zaručený elektronický podpis je platný a jeho kvalifikovaný certifikát nebyl zneplatněn (§ 5 odst. 2 zákona) nebo elektronická značka je platná a její kvalifikovaný systémový certifikát nebyl zneplatněn (§ 5a odst. 3 zákona), případně zda je platné kvalifikované časové razítko, pokud zvláštní

---

[1]) Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů.

[2]) Například zákon č. 97/1974 Sb., o archivnictví, ve znění zákona č. 343/1992 Sb., zákona č. 27/2000 Sb., zákona č. 120/2001 Sb., zákona č. 107/2002 Sb. a zákona č. 320/2002 Sb.

právní předpis stanoví povinnost připojit jej k datové zprávě,

d) je připojen kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát podle písmene b) nebo zda je uveden akreditovaný poskytovatel certifikačních služeb, který certifikát vydal a vede jeho evidenci, a

e) kvalifikovaný certifikát obsahuje údaje, na jejichž základě je možné osobu, která podepsala datovou zprávu, jednoznačně identifikovat.

(7) Pokud elektronická podatelna zjistí, že kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát podle odstavce 6 písm. c) byly v době doručení datové zprávy neplatné, a pokud lze usuzovat, že zaručený elektronický podpis nebo elektronická značka byly vytvořeny v době platnosti tohoto certifikátu, orgán veřejné moci za účelem zjištění platnosti elektronické značky nebo zaručeného elektronického podpisu

a) ověří, zda je připojeno platné kvalifikované časové razítko podepsané nebo označené datové zprávy a zda toto razítko bylo vytvořeno před okamžikem zneplatnění certifikátu datové zprávy a zda je platné, nebo

b) uvědomí podepsanou osobu, není-li připojeno platné kvalifikované časové razítko, že nemá možnost provést veškeré úkony potřebné k tomu, aby ověřil, že zaručený elektronický podpis nebo elektronická značka jsou platné a jejich kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát nebyly zneplatněny před vytvořením zaručeného elektronického podpisu nebo elektronické značky.

(8) Úkony potřebné k ověření, že zaručený elektronický podpis je platný a jeho kvalifikovaný certifikát nebyl zneplatněn nebo že elektronická značka je platná a její kvalifikovaný systémový certifikát nebyl zneplatněn nebo že kvalifikované časové razítko je platné podle odstavce 6 písm. c), jsou uvedeny v příloze k této vyhlášce.

(9) O výsledku zjištění skutečností uvedených v odstavcích 6 a 7 se při doručení do identifikátoru elektronické podatelny zaznamenávají údaje, které tyto skutečnosti dokládají.

§ 3

Odeslání datové zprávy

(1) Odesílaná datová zpráva se v elektronické podatelně ukládá do úložiště vypravených datových zpráv ve tvaru, ve kterém byla odeslána. Je-li k datové zprávě připojen uznávaný elektronický podpis oprávněného zaměstnance orgánu veřejné moci a jeho kvalifikovaný certifikát nebo uznávaná elektronická značka orgánu veřejné moci a její kvalifikovaný systémový certifikát, ukládají se spolu s datovou zprávou.

(2) Před odesláním z orgánu veřejné moci prochází datová zpráva kontrolou výskytu škodlivého kódu.

(3) Odesílaná datová zpráva se v elektronické podatelně eviduje v souladu s vnitřními předpisy orgánu veřejné moci upravujícími evidenci vypravovaných písemností s tím, že čas odeslání datové zprávy je zaznamenán s přesností na sekundu.

§ 4

Údaj, na základě kterého je možné osobu jednoznačně identifikovat

Údaj, na jehož základě je možné osobu jednoznačně identifikovat, se uvádí ve struktuře desetimístného čísla v desítkové soustavě v rozsahu 1 100 100 100 až 4 294 967 295 a je spravován ústředním orgánem státní správy. Jeho hodnota není zaměnitelná s rodným číslem a nesmí být osobním údajem podle zvláštního právního předpisu[3]).

§ 5

Účinnost

Tato vyhláška nabývá účinnosti dnem 1. ledna 2005.

Ministr:

Mlynář v. r.

[3]) § 4 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

Příloha k vyhlášce č. 496/2004 Sb.

Úkony potřebné k ověření, že zaručený elektronický podpis a elektronická značka jsou platné a jejich kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát nebyly zneplatněny, a k ověření platnosti kvalifikovaného časového razítka

1. Ověření zaručeného elektronického podpisu a elektronické značky

Ověření zaručeného elektronického podpisu podepisující osoby nebo elektronické značky označující osoby datové zprávy se provádí podle standardů asymetrických kryptografických algoritmů a kryptografických hašovacích funkcí odpovídajících schématům použitým při vytváření zaručeného elektronického podpisu. Parametrem asymetrického kryptografického algoritmu jsou data pro ověřování elektronických podpisů odpovídající datům pro vytváření elektronických podpisů, k nimž byl vydán kvalifikovaný certifikát, nebo data pro ověřování elektronických značek odpovídající datům pro vytváření elektronických značek, k nimž byl vydán kvalifikovaný systémový certifikát. Standardy kryptografických asymetrických algoritmů a kryptografických hašovacích funkcí jsou uvedeny v tabulce č. 1 a 2 této přílohy. Ověření se provádí zpravidla pomocí aplikace bez zásahu ověřující osoby.

2. Ověření platnosti certifikátu

a) Ověření intervalu doby platnosti

Ověření, zda v době doručení datové zprávy byl kvalifikovaný certifikát podepisující osoby nebo kvalifikovaný systémový certifikát označující osoby v intervalu doby platnosti. Ověření se provádí zpravidla pomocí aplikace bez zásahu ověřující osoby.

b) Ověření elektronické značky certifikátu

Ověření elektronické značky, kterou kvalifikovaný poskytovatel označil kvalifikovaný certifikát podepisující osoby nebo kvalifikovaný systémový certifikát označující osoby, obdobně jako se ověřuje elektronická značka datové zprávy podle bodu 1. Ověření se provádí zpravidla pomocí aplikace bez zásahu ověřující osoby.

c) Ověření, zda certifikát nebyl zneplatněn

Ověření, zda se kvalifikovaný certifikát podepisující osoby nebo kvalifikovaný systémový certifikát označující osoby nenacházejí v seznamu zneplatněných certifikátů s časem zneplatnění, který předchází času doručení datové zprávy. Rozhodným seznamem zneplatněných certifikátů je pro tyto účely seznam, jehož platnost začíná bezprostředně po čase doručení datové zprávy. Ověření provádí ověřující osoba, aplikace jej zpravidla neprovádí.

d) Ověření elektronické značky seznamu zneplatněných certifikátů

Ověření elektronické značky, kterou kvalifikovaný poskytovatel označil seznam zneplatněných certifikátů, se provádí obdobně jako se ověřuje elektronická značka datové zprávy podle bodu 1.

e) Certifikační cesta

Elektronická značka kvalifikovaného certifikátu podepisující osoby nebo kvalifikovaného systémového certifikátu označující osoby je založena na kvalifikovaném systémovém certifikátu poskytovatele. I ten může být označen elektronickou značkou poskytovatele, která je založena na dalším kvalifikovaném systémovém certifikátu poskytovatele. Tento vztah mezi certifikáty se označuje pojmem certifikační cesta. Pro ověření platnosti certifikátu označující nebo podepisující osoby je nutné provést ověření platnosti všech certifikátů v certifikační cestě podle písm. a) až d) tohoto bodu. Certifikační cesta je vyznačena v každém vydaném certifikátu.

3. Ověření kvalifikovaného časového razítka

Ověření elektronické značky kvalifikovaného časového razítka obdobně, jako se ověřuje elektronická značka datové zprávy podle bodu 1.

Ověření platnosti kvalifikovaného systémového certifikátu, na kterém je založena elektronická značka kvalifikovaného časového razítka, obdobně jako se ověřuje platnost certifikátu podle bodu 2.

Tabulka č. 1

Index asymetrického algoritmu	Zkratka kryptografického asymetrického algoritmu	Normativní odkazy
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]

Normativní dokumenty:
[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.

Tabulka č. 2

Index hashovací funkce	Zkratka kryptografické hashovací funkce	Normativní odkazy
2.01	sha1	[5,6]
2.02	ripemd160	[5]

Normativní dokumenty:
[5] ISO/IEC 10118-3: Information technology - Security techniques - Hash functions - Part 3: Dedicated hash functions.
[6] NIST: FIPS Publication 180-1: Secure Hash Standard (SHS-1).