

# TEZE PROVÁDĚCÍCH PRÁVNÍCH PŘEDPISŮ

## I.

**Vyhláška, kterou se mění vyhláška č. 645/2004 Sb., kterou se provádějí některá ustanovení zákona o archivnictví a spisové službě a o změně některých zákonů, ve znění vyhlášky č. 192/2009 Sb.**

### A. Účel právní úpravy

Návrh vyhlášky, kterou se mění vyhláška č. 645/2004 Sb., kterou se provádějí některá ustanovení zákona o archivnictví a spisové službě a o změně některých zákonů, ve znění vyhlášky č. 192/2009 Sb., (dále jen „návrh vyhlášky“) je právní úpravou, která reaguje na dva zásadní legislativní impulsy. Tím prvním je návrh zákona, kterým se mění zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů, a další související zákony (dále jen „návrh zákona“), konkrétně změny, které tento návrh zákona přináší do oblasti péče o archiválie v digitální podobě. Druhým impulsem jsou dlouhodobé požadavky praxe na zpřesnění úpravy typů evidenčních jednotek a druhů archivních pomůcek, která v současné době již ne zcela odpovídá skutečnému stavu archiválií, resp. požadavkům na jejich evidenci.

Návrh vyhlášky proto jednak v její paragrafové části bude reakcí na terminologické úpravy z oblasti archivnictví provedené zejména v bodě 2 návrhu zákona (definice pojmu „péče o archiválie“, jehož součástí je také „uložení archiválie“) a v bodě 50 (zrušení kategorizace archiválií), jednak dosavadní znění vyhlášky č. 645/2004 Sb. doplní o podrobnosti nakládání s archiváliemi v digitální podobě, a to v rozsahu úpravy oblasti digitálního archivnictví provedené návrhem zákona.

Návrh vyhlášky současně bude naplňovat návrhem zákona nově vymezená zmocnění k úpravě podrobností v oblasti péče o archiválie, a to konkrétně na doplnění § 15 odst. 1 o zmocnění k vydání prováděcího právního předpisu, kterým se stanoví náležitosti soupisu předávaných dokumentů v digitální podobě, na doplnění § 19 o zmocnění k úpravě podrobností vytváření, správy a zpřístupňování metadat archiválií a rozsahu metadat dokumentů v digitální podobě vybraných jako archiválie mimo skartační řízení u původců, kteří nevykonávají spisovou službu v elektronické podobě v elektronických systémech spisové služby, a dále na zmocnění stanovené v § 40 odst. 7 návrhu zákona pro stanovení maximální výše úhrady nákladů služeb poskytovaných veřejnými archivy, kterou jsou tyto oprávněny požadovat.

### B. Teze právní úpravy

#### 1. Terminologické změny

- 1.1 – Péče o archiválie – odraz v § 2 odst. 2, § 6, odst. 2 a 3, § 12 odst. 1 a 2, § 15 odst. 3.
- 1.2 – Zrušení kategorizace archiválií – odraz v § 4 odst. 1 písm. n), § 6 odst. 3 písm. i), § 13 odst. 1, 2, 4 a 5.
- 1.3 – Změna úpravy předkládání žádosti o nahlížení do archiválií – odraz v § 16 odst. 1.

## 2. Provedení zmocňovacích ustanovení

- 2.1 – Náležitosti soupisu předávaných dokumentů v digitální podobě:
  - 2.1.1 – stanovení identifikačních položek základní identifikace archiválie v digitální podobě,
  - 2.1.2 – stanovení náležitostí popisu archiválie v digitální podobě (údaje o zařídění a začlenění funkčního odkazu na archivní pomůcku).
  
- 2.2 – Podrobnosti vytváření, správy a zpřístupňování metadat archiválií a rozsahu metadat dokumentů v digitální podobě vybraných jako archiválie mimo skartační řízení u původců, kteří nevykonávají spisovou službu v elektronické podobě v elektronických systémech spisové služby:
  - 2.2.1 – stanovení charakteristik spravovaných metadat,
  - 2.2.2 – dokumentace elektronických systémů spisové služby,
  - 2.2.3 – ukládání spisových řádů.
  
- 2.3 – Stanovení maximální výše úhrady nákladů služeb poskytovaných veřejnými archivy:
  - 2.3.1 – návrh vyhlášky bude zahrnovat nové znění přílohy č. 4, zahrnující také nové typy služeb archivů, jako např. ověřování shody mezi uloženou archiválií v digitální podobě a zhotovenou replikou, provádění vyhledávání a zpracovávání rešerší, popřípadě další specifické služby související s péčí archiválie v digitální podobě (viz návrh zákona).
  - 2.3.2 – v příloze č. 4 dále budou zohledněny nové typy služeb archivů, které souvisejí s rozvojem zpracovatelských technologií, nabídkou služeb prostřednictvím výpočetní techniky apod. tak, jak jsou známy z dosavadních zkušeností archivů, a tak, jak vycházejí z potřeb uživatelů.

## 3. Další podrobnosti archivní péče o archiválie v digitální podobě

- 3.1 – Text vyhlášky č. 645/2004 Sb. bude podroben analýze efektivnosti jejích jednotlivých ustanovení tak, aby byly odstraněny požadavkům praxe nevyhovující úpravy, případné rozpory s jinými právními předpisy a aby naopak normativní text byl doplněn o podrobnosti svědčící reálným důsledkům rozvoje právních vztahů v oblasti archivní péče.
- 3.2 – Rozšíření rozsahu archivy poskytovaných služeb – zahrnuto do vzorového badatelského řádu.
- 3.3 – Zpřesnění charakteristik a popisu evidenčních jednotek v příloze č. 1.
- 3.4 – Zpřesnění charakteristik a popisu druhů archivních pomůcek v příloze č. 2.

## II. Vyhláška o podrobnostech výkonu spisové služby

### A. Účel právní úpravy

Ustanovením § 70 odst. 1 zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění zákona č. 190/2009 Sb., je Ministerstvo vnitra zmocněno k vydání prováděcího právního předpisu, který se stanoví podrobnosti výkonu spisové služby. Právním předpisem vydaným na základě tohoto zmocnění je vyhláška č. 191/2009 Sb., o podrobnostech výkonu spisové služby, která – ačkoliv vydaná s účinností od 1. července 2009 – ve vztahu k návrhu zákona, kterým se mění zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů, a další související zákony, není předpisem splňujícím požadavky na kompletní a systematickou úpravu podrobností výkonu spisové služby ve smyslu citovaného zmocnění. Pokud by citovaná vyhlášky takovým předpisem měla být, musela by, a to i s přihlédnutím k potřebě doplnit jednotlivá ustanovení o upřesnění podmínek nakládání s dokumenty v digitální podobě, zejména pak v oblasti příjmu dokumentů a jednotné úpravy režimu adres elektronické podatelny, být rozsáhlým způsobem upravena, a to především ve smyslu jejího doplnění. Taková úprava by však nesvědčila požadavku uživatelské přehlednosti, kladenému na systematiku právního předpisů, a proto bude zpracován prováděcí předpis nový, nahrazující současnou vyhlášku č. 191/2009 Sb. Struktura nové vyhlášky o podrobnostech výkonu spisové služby je zamýšlena v rozsahu dále uvedených tezí.

### B. Teze připravované právní úpravy

#### I. Příjem dokumentů

[§ 70 odst. 1 písm. a) zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů]

Prvním okruhem právních vztahů, který bude nejvíce podstatnou a nejobsáhlejší změnou v nové vyhlášce upravující podrobnosti výkonu spisové služby, je příjem dokumentů. Podrobnosti příjmu dokumentů budou upraveny komplexně, tedy včetně převzetí předmětu právní úpravy vyhlášky č. 496/2004 Sb., o elektronických podatelkách, a 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. Společně s úpravou podrobností vlastního výkonu spisové služby se vyhláška bude rovněž věnovat sjednocení terminologie používané v této oblasti a jednoznačnému obsahovému vymezení užívaných pojmů, a to především pojmu dokument a jeho zpracovatelským podobám.

*Úprava příjmu dokumentů bude zahrnovat oblasti:*

#### 1. Podatelna

##### 1.1 Příjem dokumentů v digitální podobě:

###### 1.1.1 Podmínky provozování adresy elektronické podatelny

Úpravou budou stanoveny porobnosti příjmu dokumentů v digitální podobě prostřednictvím adresy elektronické podatelny umožňující přijímat dokumenty v digitální podobě bez ohledu na způsob jejich doručení (zejména veřejnou sítí internet, informačním systémem datových schránek a na přenosném nosiči).

- 1.1.2 Okamžik doručení dokumentu v digitální podobě, potvrzení přijetí dokumentu.
- 1.1.3 Kontrola doručených dokumentů v digitální podobě, nakládání s dokumenty obsahujícími škodlivý kód.
- 1.1.4 Kontrola datových formátů dokumentů (§ 64 odst. 1 zákona č. 499/2004 Sb. – *zajištění příjmu dokumentů v digitální podobě alespoň v zákonem stanovených datových formátech pro příjem dokumentů v digitální podobě*).
- 1.1.5 Kontrola integrity a autentičnosti doručeného dokumentu v digitální podobě, ověření platnosti (struktura údajů) elektronického podpisu, elektronické značky nebo kvalifikovaného časového razítka.  
Stanovení podmínek identifikace adresáta (podání zasláná prostřednictvím e-podatelny musí obsahovat základní identifikaci odesílatele, tedy zejména jeho jméno, popřípadě jména, příjmení a adresu pobytu na území České republiky, popřípadě bydliště v cizině v případě právnické osoby název nebo obchodní firmu a sídlo).
- 1.1.6 Úložiště doručených dokumentů v digitální podobě, zavedení dokumentu v digitální podobě do elektronického systému spisové služby a označení jednoznačným identifikátorem.

## 1. 2 Příjem dokumentů v analogové podobě:

- 1.2.1 Doručení dokumentu v analogové podobě.
- 1.2.2 Opatřování dokumentů prezentačním - podacím razítkem.
- 1.2.3 Obálka.
- 1.2.4 Dokumenty neúředního charakteru.

## 1.3 Převádění dokumentů z digitální podoby do podoby analogové a naopak:

- 1.3.1 Podmínky převodu, využití autorizované konverze dokumentů.
- 1.3.2 Zachování věrohodnosti dokumentů.

## **2. Označování a evidence dokumentů**

### 2. 1 Označování dokumentů:

[§ 70 odst. 1 písm. b) zákona č. 499/2004 Sb.]

- 2.1.1 Postupy původce při vedení spisové služby v elektronické podobě a v listinné podobě.
- 2.1.2 Obsah otisku podacího razítka.
- 2.1.3 Převod dokumentu v analogové podobě na dokument v digitální podobě a opačně.
- 2.1.4 Úložiště převedených dokumentů; povinnost ukládat doručené dokumenty i po jejich převedení.

### 2. 2 Evidence dokumentů:

[§ 70 odst. 1 písm. b) zákona č. 499/2004 Sb.]

#### 2.2.1 Elektronický systém spisové služby a podací deník.

Podací deník:

- a) vlastnosti podacího deníku; vedení zkratk použitých v podacím deníku,
  - b) údaje o dokumentu v podacím deníku nebo v elektronickém systému spisové služby,
  - c) přeevidování dokumentů,
  - d) evidenční řada dokumentů, uzavření podacího deníku,
  - e) samostatné evidence dokumentů, evidenční informační systémy, vazby k dalším informačním systémům a jejich uživatelské požadavky,
  - f) povaha a účel jednoznačného identifikátoru.
- 2.2.2 Číslo jednací a evidenční číslo ze samostatné evidence dokumentů:
- a) tvar čísla jednacího,
  - b) tvar evidenčního čísla ze samostatné evidence dokumentů.
2. 2. 3 Sběrný arch:
- a) obsahové náležitosti,
  - b) podmínky zpracovávání.

## **3. Tvorba spisu**

### 3. 1 Tvorba spisu:

- 3.1.1 Základní způsoby tvorby spisu, postup.
- 3.1.2 Spisová značka.
- 3.1.3 Obsah spisu, uspořádání dokumentů.

### 3.2 Vedení jmenných rejstříků a využívání údajů v nich vedených.

[§ 70 odst. 1 písm. c) zákona č. 499/2004 Sb.]

### 3.3 Rozdělování a oběh dokumentů.

[§ 70 odst. 1 písm. d) a e)]

### 3.4 Činnost podatelny a součástí původce v systému rozdělování dokumentů a jejich vnitřního oběhu v rámci původce.

## **II. Vyřizování dokumentů**

### **1. Vyřizování dokumentů jako součást odborné správy dokumentů**

#### 1. 1 Vyřizování dokumentů - obecné požadavky:

[§ 70 odst. 1 písm. f) zákona č. 499/2004 Sb.]

- 1.1.1 Způsob vyřizování dokumentů.
- 1.1.2 Druhy vyřízení dokumentů.
- 1.1.3 Připojení spisového znaku, skartačního znaku a skartační lhůty, popřípadě roku zařazení dokumentu do skartačního řízení.
- 1.1.4 Záznam o vyřízení v evidenci dokumentů.

#### 1. 2. Spisový znak, skartační znak a skartační lhůta:

- 1.2.1 Spisový a skartační plán, struktura, podrobnosti ohledně přípravy a užívání [§ 66 odst. 6, § 70 odst. 1 písm. k) ].
- 1.2.2 Skartační znak, charakteristika.
- 1.2.3 Skartační lhůta, charakteristika, spouštěcí událost, maximální délka.
- 1.2.4 Skartační lhůta a spis.

#### 1. 3 Vyhотовování dokumentů:

[§ 70 odst. 1 písm. g) zákona č. 499/2004 Sb.]

- 1.3.1 Vyhотовování dokumentů.
- 1.3.2 Náležitosti vyhotovovaného dokumentu.

#### 1. 4 Podepisování dokumentů a užívání úředních razítek:

[§ 70 odst. 1 písm. h) zákona č. 499/2004 Sb.]

- 1.4.1 Uvedení termínu „podpis“ současně se jménem a příjmením.
- 1.4.2 Podmínky podepisování dokumentů v analogové podobě, podmínky používání uznávaného elektronického podpisu, uznávané elektronické značky, kvalifikovaného časového razítka, datových schránek a úředních razítek.
- 1.4.3 Evidence úředních razítek, její charakteristika.
- 1.4.4 Ztráta úředního razítka.
- 1.4.5 Evidence kvalifikovaných certifikátů vydaných akreditovanými poskytovateli certifikačních služeb a kvalifikovaných systémových certifikátů, rozsah evidence.

## **2. Odesílání dokumentů**

### 2.1 Úkoly podatelny (výpravna):

- 2.1.1 Odesílání dokumentů v analogové podobě.
- 2.1.2 Odesílání dokumentů v digitální podobě (elektronické elektronická podatelna, datová schránka).
- 2.2.3 Převod dokumentů z analogové podoby do podoby digitální a naopak.

## 2.2 Údaje zaznamenávané o odeslání dokumentu v příslušné evidenci dokumentů:

2.2.1 Dokumenty v analogové podobě.

2.2.2 Dokumenty v digitální podobě (využití funkcionalit elektronických systémů spisové služby).

## **3. Ukládání dokumentů**

### 3.1 Spisovna.

### 3.2 Kontrola úplnosti dokumentů.

### 3.3 Evidence uložených dokumentů a spisů, její obsah.

### 3.4 Zapůjčování a nahlížení do dokumentů.

### 3.5 Poškození nebo zničení dokumentu.

## **4. Vyřazování dokumentů**

### 4.1 Postup při vyřazování dokumentů a podrobnosti skartačního řízení: [§ 9 odst. 2, § 70 odst. 1 písm. l) zákona č. 499/2004 Sb.]

4.1.1 Vlastnosti dokumentů a úředních razítek zařazovaných do skartačního řízení.

4.1.2 Doplnění chybějících metadat.

Podle ustanovení § 13 odst. 4 zákona č. 499/2004 Sb. se to týká zejména dokumentů vzniklých z činnosti soukromoprávních původců bez povinnosti vést spisovou službu.

Doplnění se týká následujících metadat:

- a) datum doručení nebo vzniku dokumentu,
- b) identifikace odesílatele,
- c) datum ze dne (je-li uvedeno),
- d) číslo jednacích (je-li uvedeno),
- e) jazyk,
- f) stručný obsah (věc),
- g) údaje o evidenci a vyřizování, byly-li zaznamenány,
- h) spisový znak se skartačním znakem a skartační lhůtou (byly-li přiděleny),
- i) název archivního souboru, do něhož bude dokument zařazen,
- j) datový formát,
- k) velikost dokumentu v bytech,
- l) použitý software.

4.1.3 Dokumenty obsahující utajované informace.

4.1.4 Stanovení způsobu přípravy a průběh skartačního řízení.

4.1.5 Seznamy dokumentů určených k posouzení ve skartačním řízení, jejich náležitosti.

4.1.6 Skartační návrh na vyřazení dokumentů, popřípadě razítek, činnost příslušného archivu.

4.1.7 Protokol o provedeném skartačním řízení, jeho náležitosti.

- 4.1.8 Předání dokumentů vybraných jako archiválie, náležitosti úředního záznamu o předání.
- 4.1.9 Náležitosti soupisu předávaných dokumentů v digitální podobě vybraných jako archiválie (§ 15 odst. 1 zákona č. 499/2004 Sb.).
- 4.1.10 Souhlas ke zničení dokumentů a úředních razítek, zabezpečení jejich zničení, vymezení pojmu zničení.
- 4.1.11 Postup při vytváření repliky dokumentu v digitální podobě vybraného jako archiválie v datovém formátu stanoveném prováděcím právním předpisem a způsob jejího předání Národnímu archivu nebo digitálnímu archivu k uložení [§ 25 odst. 1 písm. b) zákona č. 499/2004 Sb.].

#### 4.2 Vyřazování dokumentů mimo skartační řízení.

#### 4.3 Spisová rozluka:

[§ 70 odst. 1 písm. o) zákona č. 499/2004 Sb.]

- 4.3.1 Důvod provedení spisové rozluky.
- 4.3.2 Předávací seznamy vyřízených dokumentů a uzavřených spisů, náležitosti.
- 4.3.3 Předávací seznamy nevyřízených dokumentů a neuzavřených spisů, náležitosti, postup přebírajícího původce/nástupce.

### **III. Datové formáty a převody dokumentů**

#### 3. 1 Vstupní datové formáty:

[§ 64 odst. 1 a § 70 odst. 1 písm. n) zákona č. 499/2004 Sb. ]

- 3.1.1 Obecná charakteristika.
- 3.1.2 Popis jednotlivých formátů.
- 3.1.3 Výběr dalších formátů podle potřeb původce a způsob jejich zveřejňování.

#### 3. 2 Výstupní datové formáty:

[§ 70 odst. 1 písm. m)]

- 3.2.1 Obecná charakteristika.
- 3.2.2 Popis jednotlivých formátů.
- 3.2.3 Použití dalšího datového formátu.
- 3.2.4 Výstupní datový formát metadat.

#### 3.4 Stanovení podrobností o údajích v doložce související s převedením nebo změnou datového formátu dokumentu.

[§ 69a odst. 7, § 70 odst. 1 písm. q) zákona č. 499/2004 Sb.]

### **IV. Vedení spisové služby v mimořádných situacích**

Dosavadní úprava této problematiky provedená v § 21 vyhlášky č. 191/2009 Sb., o podrobnostech výkonu spisové služby, se v praxi ukázala jako účelná, a proto se předpokládá ponechat její obsah s drobnými upřesněními zpracovanými na základě zkušeností s dosavadním využíváním tohoto ustanovení. Jako mimořádné situace budou i do budoucna označeny „živelní pohromy, ekologické, průmyslové nebo jiné havárie, anebo v případě jiné mimořádné situace, v jejichž důsledku je původci znemožněno

po omezené časové období užívání jím vykonávané spisové služby „obvyklým způsobem“. S přihlédnutím k charakteru uvedených situací bude stanovena povinnost vést spisovou službu v daném časovém období v listinné podobě v podacím deníku, a to za podmínek stanovených původcem ve spisovém řádu nebo v jiném vnitřním předpise upravujícím výkon spisové služby.

*Předmětem úpravy podrobností výkonu spisové služby budou:*

4.1 Charakteristika, důvody vzniku mimořádné situace.

4.2 Náhradní evidence.

4.3 Ukládání dokumentů evidovaných a vyřízených v náhradní evidenci.

### **III.**

**Vyhláška o struktuře údajů, na základě kterých je možné osobu jednoznačně identifikovat, a postupu při ověřování platnosti zaručeného elektronického podpisu, elektronické značky a kvalifikovaného časového razítka**

#### **§ 1**

**Údaj, na základě kterého je možné osobu jednoznačně identifikovat**

Údajem, na jehož základě je možné osobu jednoznačně identifikovat, je ....

#### **§ 2**

**Postup při ověřování platnosti zaručeného elektronického podpisu, elektronické značky a kvalifikovaného časového razítka**

(1) 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 jsou uvedeny v příloze k této vyhlášce.

(2) Okamžikem, ke kterému je ověřována platnost kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu, je okamžik doručení datové zprávy.

(3) Pokud je k podepsané datové zprávě připojeno platné kvalifikované časové razítko a není-li kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát v okamžiku doručení datové zprávy platný, ověřuje se jeho platnost k okamžiku uvedenému v kvalifikovaném časovém razítku.

(4) Okamžikem, ke kterému je ověřována platnost kvalifikovaného systémového certifikátu, na kterém je založena elektronická značka kvalifikovaného časového razítka, je okamžik ověřování časového razítka. Není-li uvedený certifikát v tomto okamžiku platný, ověřuje se vzhledem k času uvedenému v tomto časovém razítku.

## Příloha

**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 okamžiku, ke kterému je platnost certifikátu ověřována, 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 kvalifikovaný certifikát podepisující osoby nebo kvalifikovaný systémový certifikát označující osoby nebyl v okamžiku, ke kterému je posuzována jeho platnost, zneplatněn. Kontrola zneplatnění certifikátu se provádí v souladu s certifikační politikou poskytovatele certifikačních služeb, který certifikát vydal. Je-li pro toto ověření využíván seznam zneplatněných certifikátů, je pro tyto účely rozhodným seznamem 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.

#### e) Certifikační cesta

Elektronická značka kvalifikovaného certifikátu podepisující osoby nebo kvalifikovaného systémového certifikátu označující osoby je založena na kvalifikovaném

systemovém certifikátu poskytovatele. I ten může být označen elektronickou značkou poskytovatele, která je založena na dalším kvalifikovaném systemovém 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 systemového 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	sha-1		[5,6]
2.02	sha-256		[5,6]
2.03	sha-384		[5,6]
2.04	sha-512		[5,6]
2.03	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).