# VYHLÁŠKA č. 378/2006 Sb.

## ze dne 19. července 2006 o postupech kvalifikovaných poskytovatelů certifikačních služeb, o požadavcích na nástroje elektronického podpisu a o požadavcích na ochranu dat pro vytváření elektronických značek (vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb)

Ministerstvo informatiky (dále jen „ministerstvo“) stanoví podle § 20 odst. 1, 2, 3 a 5 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. a zákona č. 440/2004 Sb., (dále jen „zákon“):

## ČÁST PRVNÍ

## OBECNÁ USTANOVENÍ

### § 1

### Předmět úpravy

(1) Tato vyhláška stanoví

a) způsob splnění informační povinnosti podle § 6 odst. 1 písm. a) a f) a odst. 3 zákona, kvalifikační požadavky podle § 6 odst. 1 písm. b) zákona, požadavky na bezpečné systémy a bezpečné nástroje podle § 6 odst. 1 písm. c) a d) zákona, způsob uchovávání informací a dokumentace podle § 6 odst. 5 a 6 zákona a způsob, jakým se splnění těchto požadavků dokládá,

b) způsob zajištění bezpečnosti seznamů podle § 6a odst. 1 písm. e) a f) zákona, určení data a času podle § 6a odst. 1 písm. g) zákona, náležitosti opatření podle § 6a odst. 1 písm. h) zákona, způsob splnění informační povinnosti podle § 6a odst. 1 písm. i) zákona, způsob ochrany a zajištění souladu dat podle § 6a odst. 2 zákona, způsob zneplatnění certifikátů podle § 6a odst. 3 a 4 zákona a způsob, jakým se splnění těchto požadavků dokládá,

c) způsob zajištění přesnosti času při vytváření kvalifikovaného časového razítka podle § 6b odst. 1 písm. b) zákona, způsob zajištění souladu dat podle § 6b odst. 1 písm. c) zákona, náležitosti opatření podle § 6b odst. 1 písm. d) zákona, způsob splnění informační povinnosti podle § 6b odst. 1 písm. e) zákona a způsob, jakým se splnění těchto požadavků dokládá,

d) způsob zajištění postupů, které musí podporovat prostředky pro bezpečné vytváření elektronických podpisů při ochraně dat pro vytváření elektronických podpisů podle § 17 zákona a prostředky pro vytváření elektronických značek při ochraně dat pro vytváření elektronických značek podle § 17a zákona, a způsob, jakým se splnění těchto požadavků dokládá.

(2) Tato vyhláška byla oznámena v souladu se směrnicí Evropského parlamentu a Rady 98/34/ES ze dne 22. června 1998 o postupu poskytování informací v oblasti technických norem a předpisů a pravidel pro služby informační společnosti, ve znění směrnice 98/48/ES.

§ 2

**Vymezení některých pojmů**

Pro účely této vyhlášky se rozumí

a) nadřízenými kvalifikovanými systémovými certifikáty kvalifikované systémové certifikáty, které obsahují data pro ověřování elektronických značek odpovídající datům pro vytváření elektronických značek, kterými poskytovatel označuje vydávané kvalifikované certifikáty, kvalifikované systémové certifikáty, seznamy podle § 6a odst. 1 písm. f) zákona a vydávaná kvalifikovaná časová razítka,
b) seznamem vydaných certifikátů seznam, který má náležitosti podle § 6a odst. 1 písm. e) zákona a splňuje požadavky této vyhlášky,
c) seznamem zneplatněných certifikátů seznam, který má náležitosti podle § 6a odst. 1 písm. f) zákona a splňuje požadavky této vyhlášky,
d) bezpečnostní dokumentací soubor dokumentů, které poskytovatel vytváří v souladu s touto vyhláškou a ve kterých stanoví zásady a veškeré postupy uplatňované při zajišťování kvalifikovaných certifikačních služeb,
e) bezpečným kryptografickým modulem nástroj elektronického podpisu, který poskytovatel používá pro činnosti stanovené touto vyhláškou a který splňuje požadavky této vyhlášky,
f) kritickými činnostmi poskytovatele příjem žádostí o zneplatnění certifikátů, zneplatnění certifikátů a vydání seznamu zneplatněných certifikátů, případně další činnosti, které poskytovatel určí při analýze rizik jako kritické činnosti,
g) mimořádnou událostí událost, která ohrožuje poskytování kvalifikovaných certifikačních služeb a nastává zejména v důsledku selhání důvěryhodného systému, technického zařízení, a nebo výskytu faktoru, který není pod kontrolou poskytovatele,
h) nejistotou časového údaje možné odchýlení měřidla času od světového koordinovaného času v součtu s nejistotou měření časového údaje.

ČÁST DRUHÁ

## POSTUPY KVALIFIKOVANÝCH POSKYTOVATELŮ CERTIFIKAČNÍCH SLUŽEB A OCHRANA DAT PRO VYTVÁŘENÍ ELEKTRONICKÝCH ZNAČEK

HLAVA PRVNÍ

### Postupy poskytovatelů

§ 3

**Požadavky na bezpečné systémy**

Systémy podle § 6 odst. 1 písm. c) a d) zákona (dále jen „důvěryhodné systémy“) jsou bezpečné a bezpečnost postupů, které tyto systémy podporují, je dostačující, pokud kvalifikovaný poskytovatel certifikačních služeb (dále jen „poskytovatel“)

a) používá důvěryhodné systémy a postupy, které splňují požadavky standardu pro tyto systémy, který je uveden v bodu 1 přílohy č. 1 této vyhlášky, a požadavky českých technických norem uvedených v bodech 2 a 3 přílohy č. 1 této vyhlášky; požadavky těchto standardů a českých technických norem stanovené pro důvěryhodné systémy používané pro vydávání a správu kvalifikovaných certifikátů se použijí obdobně pro důvěryhodné systémy používané pro vydávání a správu kvalifikovaných systémových certifikátů,

b) při řízení bezpečnosti důvěryhodných systémů postupuje podle české technické normy uvedené v bodu 4 přílohy č. 1 této vyhlášky a má zaveden a uplatňuje systém řízení bezpečnosti informací podle české technické normy uvedené v bodu 5 přílohy č. 1 této vyhlášky,
c) užívá prostory, ve kterých je zajišťováno vytváření kvalifikovaných certifikátů nebo kvalifikovaných systémových certifikátů, kvalifikovaných časových razítek, prostředků pro vytváření elektronických podpisů, zneplatňování kvalifikovaných certifikátů nebo kvalifikovaných systémových certifikátů, vytváření seznamů zneplatněných certifikátů, veškeré nakládání s daty pro vytváření elektronických značek a jim odpovídajícími daty pro ověřování elektronických značek poskytovatele, nakládání s kvalifikovaným systémovým certifikátem poskytovatele a vytváření záznamů o událostech s těmito činnostmi spojených, zabezpečené obdobně jako zabezpečené oblasti kategorie „Důvěrné“ podle zvláštního právního předpisu[1)] a je zpracována dokumentace stanovená tímto právním předpisem,
d) má zpracovánu a průběžně aktualizuje bezpečnostní dokumentaci,
e) postupuje v souladu se zásadami a postupy uvedenými v bezpečnostní dokumentaci,
f) provádí kontrolu bezpečnostní shody podle této vyhlášky,
g) provádí audit systému řízení bezpečnosti informací podle této vyhlášky.

§ 4

**Bezpečnostní dokumentace**

(1) Není-li uvedeno jinak, splnění povinností stanovených zákonem a požadavků stanovených touto vyhláškou dokládá poskytovatel prostřednictvím bezpečnostní dokumentace.

(2) Bezpečnostní dokumentaci tvoří tyto dokumenty:

a) certifikační politika pro vydávání kvalifikovaných certifikátů, pokud poskytovatel tuto službu zajišťuje,
b) certifikační politika pro vydávání kvalifikovaných systémových certifikátů, pokud poskytovatel tuto službu zajišťuje,
c) politika pro vydávání kvalifikovaných časových razítek, pokud poskytovatel tuto službu zajišťuje,
d) politika pro vydávání prostředků pro bezpečné vytváření elektronických podpisů, pokud poskytovatel tuto službu zajišťuje,
e) certifikační politiky pro vydávání nadřízených kvalifikovaných systémových certifikátů,
f) zprávy pro uživatele služeb uvedených v písmenech a) až d), pokud tyto služby poskytovatel poskytuje,
g) certifikační prováděcí směrnice nebo jiné prováděcí směrnice ke službám podle písmen a) až e),
h) celková bezpečnostní politika,
i) systémová bezpečnostní politika,
j) plán pro zvládání krizových situací a plán obnovy,
k) další dokumenty poskytovatele, na které je v dokumentech podle písmen a) až j) odkazováno nebo které obsahují podrobná pravidla a podrobné postupy, kterými poskytovatel zajišťuje bezpečnost poskytovaných kvalifikovaných certifikačních služeb; z bezpečnostní dokumentace musí být zřejmé, jaké postupy poskytovatel uplatňuje při zajištění bezpečnosti systémů podle § 6 odst. 1 písm. c) a d) zákona.

---

1) Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků.

§ 5

**Obsah bezpečnostní dokumentace**

(1) Obsahem politik podle § 4 odst. 2 písm. a) až d) je vždy

a) stanovení zásad, které poskytovatel uplatňuje při zajišťování kvalifikované certifikační služby,
b) v případě vydávání kvalifikovaných certifikátů nebo kvalifikovaných systémových certifikátů popis vlastností dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek a jim odpovídajících dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek, která vytváří osoba žádající o vydání certifikátu nebo která vytváří poskytovatel a k nimž má být příslušný certifikát vydán; kryptografické algoritmy a jejich parametry, které mohou být pro tato data použity, zveřejňuje ministerstvo na své úřední desce,
c) v případě vydávání kvalifikovaných časových razítek
   1. kryptografické algoritmy, které mohou být použity při vytváření otisku dat, která mají být označena kvalifikovaným časovým razítkem a parametry těchto algoritmů,
   2. přesnost času v časovém razítku ve vztahu ke světovému koordinovanému času.

(2) Obsahem zprávy pro uživatele podle § 4 odst. 2 písm. f) jsou informace o identifikačních údajích poskytovatele a základní přehled o dané kvalifikované certifikační službě a jejím využívání.

(3) Obsahem prováděcí směrnice podle § 4 odst. 2 písm. g) je vždy stanovení postupů, které poskytovatel uplatňuje při zajišťování jednotlivých kvalifikovaných certifikačních služeb.

(4) Obsahem celkové bezpečnostní politiky podle § 4 odst. 2 písm. h) je vždy stanovení cílů a popis způsobu zabezpečení důvěryhodných systémů poskytovatele a specifikace zásad a předpisů vztahujících se k řešení bezpečnosti v důvěryhodných systémech a určení pravomocí a odpovědností za řešení bezpečnosti.

(5) Systémová bezpečnostní politika podle § 4 odst. 2 písm. i) je zpracovávána na základě provedené analýzy rizik spjatých s provozováním důvěryhodných systémů. V analýze rizik poskytovatel definuje aktiva těchto systémů, hrozby, které na ně působí, zranitelná místa systémů, pravděpodobnost výskytu hrozeb, odhad jejich následků a určuje odpovídající bezpečnostní opatření.

(6) Obsahem systémové bezpečnostní politiky je vždy

a) stanovení cílů při ochraně informací,
b) stanovení způsobu zajištění bezpečnosti,
c) určení pravomocí a odpovědností při provozování důvěryhodných systémů,
d) pravidla a postupy konkrétně definující způsob správy a ochrany informačních technologií, aktiv informačních systémů a způsob distribuce informací v rámci důvěryhodných systémů a jiných systémů, které mají s důvěryhodnými systémy vazby,
e) způsoby uplatnění celkové bezpečnostní politiky ve vztahu k provozování důvěryhodných systémů,
f) popis důvěryhodných systémů, jejich vnitřních, vnějších a vzájemných vazeb,
g) vyhodnocení analýzy rizik a popis bezpečnostních opatření podle odstavce 5,
h) způsob šíření časového údaje v rámci důvěryhodných systémů, pokud poskytovatel poskytuje službu vydávání kvalifikovaných časových razítek.

(7) Plán pro zvládání krizových situací podle § 4 odst. 2 písm. j) obsahuje vždy stanovení postupů, které jsou uplatněny v případě výskytu mimořádné události.

(8) Plán obnovy podle § 4 odst. 2 písm. j) obsahuje strategie obnovy důvěryhodných systémů, které je nutno realizovat pro

a) zachování kritických činností poskytovatele v nejkratším možném čase,
b) obnovu řádné funkce důvěryhodných systémů.

§ 6

**Požadavky na zpracování bezpečnostní dokumentace**

(1) Struktura certifikační politiky podle § 4 odst. 2 písm. a), b) a e) a certifikační prováděcí směrnice podle § 4 odst. 2 písm. g) je uvedena v příloze č. 2 této vyhlášky.

(2) U položek struktury uvedené v příloze č. 2 této vyhlášky, které se při zpracování bezpečnostní dokumentace nepoužijí, protože poskytovatel předmětnou činnost nevykonává, bude tato skutečnost uvedena.

(3) Při zpracování dokumentů celková bezpečnostní politika podle § 4 odst. 2 písm. h) a systémová bezpečnostní politika podle § 4 odst. 2 písm. i) se postupuje dle požadavků českých technických norem uvedených v bodech 4 a 6 přílohy č. 1 této vyhlášky.

§ 7

**Zveřejňování dokumentů**

(1) Poskytovatel zveřejňuje dokumenty uvedené v § 4 odst. 2 písm. a) až d) a f) v plném rozsahu.

(2) Poskytovatel může zveřejnit certifikační prováděcí směrnici nebo jiné prováděcí směrnice podle § 4 odst. 2 písm. g) v rozsahu, který neohrozí bezpečnost zajišťovaných služeb.

(3) Zveřejněním podle odstavců 1 a 2 se rozumí zveřejnění způsobem umožňujícím dálkový přístup a v prostorách, kde dochází ke kontaktu s uživateli.

§ 8

**Kontrola bezpečnostní shody**

(1) Cílem kontroly bezpečnostní shody podle § 3 písm. f) je ověření, že

a) poskytovatel provozuje důvěryhodné systémy v souladu se zákonem a s touto vyhláškou,
b) poskytovatel provádí změny v důvěryhodných systémech v souladu s bezpečnostní dokumentací poskytovatele, a to s jejími částmi upravujícími řízení změn.

(2) Předmětem kontroly bezpečnostní shody jsou

a) všechny důvěryhodné systémy poskytovatele (celková kontrola bezpečnostní shody), nebo
b) všechny změny podle odstavce 1 písm. b), které poskytovatel provedl od provedení předchozí kontroly bezpečnostní shody, a jejich vliv na důvěryhodné systémy

poskytovatele nebo ověření skutečnosti, že takové změny nenastaly (částečná kontrola bezpečnostní shody).

(3) Celková kontrola bezpečnostní shody je prováděna nejpozději do 1 roku od zahájení poskytování kvalifikovaných certifikačních služeb a následně vždy nejméně po 4 letech od předchozí celkové kontroly bezpečnostní shody, a to za předpokladu, že během těchto 4 let byly provedeny částečné kontroly bezpečnostní shody, mezi nimiž uplynul nejvíce 1 rok a první proběhla do 1 roku po celkové kontrole bezpečnostní shody.

(4) Pokud nejsou prováděny částečné kontroly bezpečnostní shody podle odstavce 2 písm. b), provádí se celkové kontroly bezpečnostní shody v intervalu nejdéle 1 roku.

(5) Kontrola bezpečnostní shody je prováděna podle požadavků české technické normy uvedené v bodu 6 přílohy č. 1 této vyhlášky.

(6) Poskytovatel zajišťuje zpracování zprávy o kontrole bezpečnostní shody, jejímž obsahem je

a) vymezení předmětu kontroly bezpečnostní shody; v případě celkové kontroly bezpečnostní shody vymezení všech důvěryhodných systémů podle odstavce 2 písm. a) s uvedením kvalifikovaných certifikačních služeb, které jsou prostřednictvím těchto systémů zajišťovány, nebo v případě částečné kontroly bezpečnostní shody vymezení změn podle odstavce 2 písm. b), které poskytovatel provedl od provedení předchozí kontroly bezpečnostní shody, a vymezení kvalifikovaných certifikačních služeb, které jsou zajišťovány prostřednictvím důvěryhodných systémů, těmito změnami ovlivněných,
b) jednoznačné určení dokumentace, která byla předmětem kontroly bezpečnostní shody;
c) popis průběhu kontroly bezpečnostní shody,
d) jméno, popřípadě jména a příjmení osoby, která provádí kontrolu bezpečnostní shody; tato osoba může být s poskytovatelem v pracovněprávním vztahu,
e) prohlášení o výsledku kontroly bezpečnostní shody, jehož součástí je prohlášení o tom, že poskytovatel provozuje důvěryhodné systémy v souladu s odstavcem 1.

(7) Pokud je v průběhu kontroly bezpečnostní shody zjištěno, že poskytovatel neprovozuje důvěryhodné systémy v souladu s odstavcem 1 písm. a) nebo neprovádí změny v důvěryhodných systémech v souladu s odstavcem 1 písm. b), musí být dosaženo nápravy, jejíž provedení je dokumentováno a v průběhu téže kontroly bezpečnostní shody ověřeno.

(8) Zprávu o kontrole bezpečnostní shody předává poskytovatel do 30 dnů od ukončení kontroly ministerstvu.

§ 9

**Audit systému řízení bezpečnosti informací**

(1) Cílem auditu systému řízení bezpečnosti informací podle § 3 písm. g) je objektivní a na poskytovateli nezávislé ověření, že je v důvěryhodných systémech poskytovatele zaveden a uplatňován systém řízení bezpečnosti informací podle české technické normy uvedené v bodu 5 přílohy č. 1 této vyhlášky.

(2) Pokud je zavedení systému řízení bezpečnosti informací v důvěryhodných systémech poskytovatele certifikováno na shodu s českou technickou normou uvedenou v bodu 5 přílohy č. 1 této vyhlášky, je provedení auditu systému řízení bezpečnosti informací považováno za splněné.

(3) Při provádění auditu systému řízení bezpečnosti informací se postupuje podle požadavků normy uvedené v bodu 7 přílohy č. 1 této vyhlášky; subjekt, který audit systému řízení bezpečnosti informací provádí, je ve vztahu k poskytovateli externí, nezávislou auditující organizací podle požadavků normy uvedené v bodu 7 přílohy č. 1 této vyhlášky.

(4) Poskytovatel poskytne subjektu, který audit systému řízení bezpečnosti informací provádí, vždy zprávu o kontrole bezpečnostní shody podle § 8 odst. 6, pokud již byla provedena, a bezpečnostní dokumentaci.

(5) Součástí zprávy o auditu systému řízení bezpečnosti informací je

a) vymezení předmětu auditu systému řízení bezpečnosti informací, přičemž vymezením předmětu auditu se rozumí vymezení kvalifikovaných certifikačních služeb, které jsou zajišťovány prostřednictvím důvěryhodných systémů,
b) jednoznačné určení dokumentace, která byla předmětem auditu systému řízení bezpečnosti informací a kterou poskytovatel poskytl subjektu, který audit systému řízení bezpečnosti informací provádí,
c) prohlášení subjektu, který audit systému řízení bezpečnosti informací provedl, o výsledku auditu systému řízení bezpečnosti informací, jehož součástí je prohlášení o splnění požadavků uvedených v odstavci 1.

(6) Pokud je v průběhu auditu systému řízení bezpečnosti informací zjištěno, že poskytovatel nezavedl a neuplatňuje v důvěryhodných systémech systém řízení bezpečnosti informací v souladu s požadavky uvedenými v odstavci 1, musí být dosaženo nápravy. Provedení nápravy musí být dokumentováno a ověřeno auditem.

(7) Poskytovatel zajistí, aby prohlášení o výsledku auditu systému řízení bezpečnosti informací bylo zveřejněno ve zprávě pro uživatele.

(8) Poskytovatel zajistí, aby audit systému řízení bezpečnosti informací byl proveden před zahájením poskytování první kvalifikované certifikační služby a následně nejméně každé 2 roky.

§ 10

**Způsob splnění informační povinnosti**

(1) Poskytovatel splní informační povinnost tím, že v dokumentech podle § 4 odst. 2 písm. a ) až d) a f) zveřejní

a) je-li právnickou osobou, firmu nebo název, právní formu a sídlo, je-li fyzickou osobou, jméno, popřípadě jména, příjmení, místo podnikání a identifikační číslo, pokud bylo přiděleno,
b) údaj o tom, zda je akreditován ministerstvem,
c) přesné podmínky pro využívání kvalifikovaných certifikačních služeb, včetně případných omezení pro jejich použití stanovených poskytovatelem, podmínky reklamací a řešení vzniklých sporů,
d) údaj o tom, kde a jakým způsobem jsou dostupné jeho nadřízené kvalifikované systémové certifikáty,
e) jakým způsobem zajišťuje poskytování informací třetím osobám podle § 6a odst. 1 písm. i) zákona, pokud předmětnou kvalifikovanou certifikační službu poskytuje, včetně kontaktních údajů, které mohou třetí osoby použít, pokud žádají o tyto informace,

a maximální dobu, která může uplynout mezi uplatněním požadavku a poskytnutím informace,

f) jakým způsobem zajišťuje poskytování informací třetím osobám podle § 6b odst. 1 písm. e) zákona, pokud předmětnou kvalifikovanou certifikační službu poskytuje, včetně kontaktních údajů, které mohou třetí osoby použít, pokud žádají o tyto informace, a maximální dobu, která může uplynout mezi uplatněním požadavku a poskytnutím této informace.

(2) Nadřízené kvalifikované systémové certifikáty podle odstavce 1 písm. d) musí být zveřejněny nejméně dvěma na sobě nezávislými způsoby, přičemž alespoň jedním z těchto způsobů je zveřejnění způsobem umožňujícím dálkový přístup.

(3) Pokud byla akreditovanému poskytovateli akreditace odňata, poskytovatel neprodleně tuto informaci

a) uvede v dokumentech podle § 4 odst. 2 písm. a) až d) a f) a zveřejní způsobem umožňujícím dálkový přístup,
b) zveřejní nejméně v jednom celostátně distribuovaném deníku stanoveném v dokumentech podle § 4 odst. 2 písm. a) až d) a f),
c) sdělí podepisujícím nebo označujícím osobám, které mají platné kvalifikované certifikáty nebo kvalifikované systémové certifikáty vydané tímto poskytovatelem, a to zasláním zprávy elektronickou poštou na elektronickou adresu, pokud ji tyto osoby uvedly v žádosti o vydání certifikátu.

(4) Součástí informace podle odstavce 3 písm. b) a c) je sdělení, že kvalifikované certifikáty vydané tímto poskytovatelem nelze nadále používat podle § 11 odst. 1 zákona a vydané kvalifikované systémové certifikáty nelze nadále používat podle § 11 odst. 2 zákona.

§ 11

**Kvalifikační požadavky**

Činnosti odpovídající rolím podle bezpečnostních požadavků standardu pro důvěryhodné systémy, který je uveden v bodu 1 přílohy č. 1 této vyhlášky, mohou vykonávat osoby, které

a) získaly vysokoškolské vzdělání v rámci akreditovaného bakalářského nebo magisterského studijního programu a mají nejméně 3 roky praxe v oblasti informačních technologií nebo středoškolské vzdělání a nejméně 5 let praxe v oblasti informačních technologií, přičemž z toho nejméně 1 rok v oblasti poskytování certifikačních služeb,
b) mají znalosti v oblasti infrastruktury veřejných klíčů a informační bezpečnosti.

§ 12

**Způsob uchovávání informací a dokumentace a náležitosti dokumentů a záznamů**

(1) Informace a dokumentace podle § 6 odst. 5 a 6 zákona musí být pořizovány, uchovávány a zpracovávány se zachováním prokazatelnosti jejich původu, dostupnosti, integrity, časové autentičnosti a důvěrnosti.

(2) Poskytovatel prostřednictvím bezpečnostní dokumentace dokládá, že

a) má identifikovány všechny typy informací a dokumentace podle § 6 odst. 5 a 6 zákona, které uchovává, a formu, ve které jsou uchovávány,
b) má identifikováno místo uložení informací a dokumentace,

c) stanovil postupy pro uchovávání informací a dokumentace a pro manipulaci s uloženými informacemi a dokumentací tak, aby byla zajištěna prokazatelnost jejich původu, dostupnost, integrita, časová autentičnost a důvěrnost v souladu s požadavky zákona a této vyhlášky,
d) stanovil postupy pro uchovávání informací a dokumentace tak, aby uložené informace a dokumentaci byl schopen doložit v zákonné lhůtě po ukončení platnosti certifikátu, ke kterému se informace a dokumentace vztahují,
e) stanovil odpovědnosti zaměstnanců, případně jiných fyzických osob, které zajišťují uchovávání informací a dokumentace, za dodržování postupů podle písmene c),
f) stanovil, jakým způsobem bude naloženo s informacemi a dokumentací po uplynutí 10 let.

(3) Pokud poskytovatel uchovává informace a dokumentaci podle § 6 odst. 5 a 6 zákona po uplynutí 10 let, prostřednictvím bezpečnostní dokumentace dokládá, že

a) má stanovenu dobu, po kterou budou informace a dokumentace uchovávány,
b) má stanoveny náležitosti uchovávání a manipulace s informacemi a dokumentací obdobně podle odstavce 2.

§ 13

**Náležitosti opatření proti zneužití a padělání certifikátů**

(1) Poskytovatel může svá data pro vytváření elektronických značek určená pro označování vydávaných kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů použít pouze pro označování těchto certifikátů a pro označování seznamu zneplatněných certifikátů.

(2) Poskytovatel zajišťuje v souladu s požadavky standardu pro důvěryhodné systémy, který je uveden v bodu 1 přílohy č. 1 této vyhlášky,

a) správu dat podle odstavce 1 v průběhu jejich životního cyklu,
b) správu dat pro ověřování svých elektronických značek odpovídajících datům podle odstavce 1 v průběhu jejich životního cyklu,
c) vytváření kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů.

(3) Činnosti podle odstavce 2

a) mohou vykonávat výhradně fyzické osoby, které jsou pro tuto činnost poskytovatelem určeny,
b) musí být vykonávány podle postupů stanovených certifikační prováděcí směrnicí,
c) musí být vykonávány v souladu se systémovou bezpečnostní politikou.

(4) Poskytovatel je povinen data pro vytváření elektronických značek podle odstavce 1 po ukončení jejich životního cyklu zničit; o tom pořizuje zápis, který obsahuje

a) popis způsobu zničení dat,
b) datum zničení dat,
c) datum pořízení zápisu,
d) jméno, popřípadě jména a příjmení a podpis osoby určené poskytovatelem k tomu, aby zničení dat provedla.

(5) Pro označování podle odstavce 1 poskytovatel používá bezpečný kryptografický modul.

(6) V případě zneužití nebo vzniku důvodné obavy ze zneužití jeho dat podle odstavce 1 poskytovatel bezodkladně

a) zneplatní kvalifikovaný systémový certifikát, který byl k těmto datům vydán,
b) zneplatní certifikát, který byl těmito daty označen,
c) zneplatní certifikát, který byl označen daty pro vytváření elektronických značek, ke kterým byl vydán certifikát podle písmene b),
d) ukončí používání dat podle odstavce 1.

(7) Pokud poskytovatel zneplatní kvalifikovaný systémový certifikát podle odstavce 6 písm. a), bezodkladně

a) zveřejní informaci o zneplatnění tohoto certifikátu s uvedením důvodu zneplatnění způsobem umožňujícím dálkový přístup, v prostorách, kde dochází ke kontaktu s uživateli, a dále nejméně v jednom celostátně distribuovaném deníku stanoveném v politice podle § 4 odst. 2 písm. a) až d),
b) informuje podepisující nebo označující osoby, které mají platné kvalifikované certifikáty nebo kvalifikované systémové certifikáty vydané tímto poskytovatelem, o zneplatnění těchto certifikátů, a to prostřednictvím zaslání zprávy elektronickou poštou na elektronickou adresu, pokud ji tyto osoby uvedly v žádosti o vydání certifikátu; součástí této informace je důvod ukončení platnosti nadřízeného kvalifikovaného systémového certifikátu poskytovatele,
c) informuje ministerstvo o zneplatnění tohoto certifikátu s uvedením důvodu zneplatnění.

§ 14

**Způsob zajištění bezpečnosti seznamů**

(1) Seznam vydaných certifikátů je bezpečný, pokud je u jednotlivých certifikátů v tomto seznamu zajištěna neporušenost.

(2) Poskytovatel označuje vydávané seznamy zneplatněných certifikátů daty pro vytváření elektronických značek podle § 13 odst. 1 a prostřednictvím bezpečného kryptografického modulu.

§ 15

**Způsob určení data a času vydání nebo zneplatnění certifikátu**

(1) Údaj o datu a času s uvedením hodiny, minuty a sekundy, kdy je kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát zneplatněn, a údaj o datu a času vydání seznamu zneplatněných certifikátů, ve kterém je záznam o zneplatněném certifikátu uveden, jsou součástí údajů o zneplatnění tohoto certifikátu v seznamu zneplatněných certifikátů; dalšími údaji jsou v případě kvalifikovaného certifikátu nejméně číslo certifikátu podle § 12 odst. 1 písm. g) zákona a v případě kvalifikovaného systémového certifikátu nejméně číslo certifikátu podle § 12a písm. f) zákona.

(2) Údaj podle odstavce 1 a údaj o datu a času vydání certifikátu jsou součástí záznamů o událostech podle § 12 odst. 2 písm. b).

(3) Synchronizace času důvěryhodných systémů s koordinovaným světovým časem musí odpovídat požadavkům standardu pro důvěryhodné systémy, který je uveden v bodu 1 přílohy č. 1 této vyhlášky.

§ 16

**Způsob ochrany dat vytvářených pro uživatele**

Poskytovatel chrání data pro vytváření elektronických podpisů, pokud je vytváří pro podepisující osobu, a zajišťuje soulad těchto dat podle požadavků standardu pro důvěryhodné systémy, který je uveden v bodu 1 přílohy č. 1 této vyhlášky; požadavky tohoto standardu stanovené pro ochranu dat pro vytváření elektronických podpisů, která poskytovatel vytváří pro podepisující osobu, se použijí obdobně pro ochranu dat pro vytváření elektronických značek, pokud je poskytovatel vytváří pro označující osobu.

§ 17

**Způsob zneplatnění certifikátů**

Poskytovatel při zajišťování zneplatňování kvalifikovaných certifikátů nebo kvalifikovaných systémových certifikátů

a) zajišťuje nepřetržitý příjem žádostí o zneplatnění kvalifikovaných certifikátů nebo kvalifikovaných systémových certifikátů, a to nejméně dvěma na sobě nezávislými způsoby,
b) zajišťuje splnění bezpečnostních požadavků na zneplatňování kvalifikovaných certifikátů podle požadavků standardu pro důvěryhodné systémy, který je uveden v bodu 1 přílohy č. 1 této vyhlášky; požadavky tohoto standardu stanovené pro zneplatňování kvalifikovaných certifikátů se použijí obdobně pro zneplatňování kvalifikovaných systémových certifikátů.

§ 18

**Způsob zajištění přesnosti určení času při vytváření kvalifikovaných časových razítek**

(1) Poskytovatel může pro určení času při vytváření kvalifikovaných časových razítek použít pouze měřidlo času, které je navázáno na světový koordinovaný čas a poskytovatel má o tom k dispozici příslušnou technickou dokumentaci.

(2) Měřidlo času je způsobilé pro zajištění přesnosti určení času podle této vyhlášky, pokud splňuje následující podmínky:

a) navázání podle odstavce 1 je opakováno v intervalech, které jsou stanoveny poskytovatelem na základě použitého druhu měřidla času, analýzy vlivů na deklarovanou nejistotu časového údaje a spolehlivosti navázání na světový koordinovaný čas,
b) je synchronizováno s koordinovaným světovým časem, a to včetně synchronizace v případě výskytu přestupné sekundy,
c) je chráněno proti hrozbám, které by mohly změnit jeho technické nebo metrologické vlastnosti zajišťované navázáním podle písmene a).

§ 19

**Způsob zajištění souladu dat v kvalifikovaných časových razítkách a náležitosti opatření proti padělání kvalifikovaných časových razítek**

(1) Poskytovatel může svá data pro vytváření elektronických značek určená pro označování vydávaných kvalifikovaných časových razítek používat pouze pro tento účel.

(2) Poskytovatel zajišťuje vydávání kvalifikovaných časových razítek, včetně implementace mechanismů, které zajistí, aby data v elektronické podobě, která jsou předmětem žádosti o vydání kvalifikovaného časového razítka, jednoznačně odpovídala datům v elektronické podobě obsaženým ve vydaném kvalifikovaném časovém razítku, v souladu

a) s požadavky standardu pro důvěryhodné systémy, který je uveden v bodu 1 přílohy č. 1 této vyhlášky, a
b) s požadavky české technické normy uvedené v bodu 3 přílohy č. 1 této vyhlášky.

(3) Poskytovatel uvede v politice pro vydávání časových razítek nejistotu časového údaje vkládaného do časového razítka. Nejistota časového údaje nesmí přesáhnout 1 sekundu.

(4) V případě výskytu události, která má vliv na bezpečnost vydání kvalifikovaného časového razítka nebo na přesnost časového údaje, který je do něj vkládán, poskytovatel

a) ihned přeruší vydávání kvalifikovaných časových razítek, a to do doby, kdy obnoví řádný stav v souladu s postupy stanovenými v plánu pro zvládání krizových situací a v plánu obnovy,
b) zveřejní informaci o této události způsobem umožňujícím dálkový přístup,
c) bez prodlení informuje o této události subjekty, se kterými má uzavřeny smluvní vztahy, které mohou být touto událostí dotčeny,
d) oznámí informaci o této události ministerstvu.

(5) Pokud událost podle odstavce 4 má vliv na již vydaná kvalifikovaná časová razítka a v důsledku toho na ně nelze spoléhat, poskytovatel zveřejní bezodkladně informaci o této události rovněž nejméně v jednom celostátně distribuovaném deníku stanoveném v politice pro vydávání kvalifikovaných časových razítek; součástí tohoto oznámení jsou údaje, na jejichž základě je možné určit, která vydaná kvalifikovaná časová razítka byla touto událostí dotčena.

(6) Při správě dat podle odstavce 1 poskytovatel postupuje obdobně jako při správě dat pro označování vydávaných kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů podle § 13 odst. 2 až 6.

(7) Predikce světové koordinované časové stupnice měřidlem času probíhá v prostorech, které jsou zabezpečeny obdobně jako zabezpečené oblasti kategorie „Důvěrné“ podle zvláštního právního předpisu.[1)]

(8) Při pořizování, uchovávání a zpracovávání dokumentace a informací souvisejících s vydáváním kvalifikovaných časových razítek poskytovatel postupuje podle § 12, přičemž typy zaznamenávaných událostí jsou specifikovány českou technickou normou uvedenou v bodu 3 přílohy č. 1 této vyhlášky.

§ 20

**Bezpečný kryptografický modul**

(1) Kryptografický modul, který poskytovatel používá pro činnosti stanovené zákonem a touto vyhláškou a který splňuje bezpečnostní požadavky na tyto moduly stanovené

a) ve standardu pro důvěryhodné systémy, který je uveden v bodu 1 přílohy č. 1 k této vyhlášce, nebo

b) ve standardu, který je uveden v bodu 11 nebo 12 přílohy č. 1 k této vyhlášce, a to minimálně pro úroveň 3,

je bezpečným kryptografickým modulem.

(2) Bezpečnost postupů, které bezpečný kryptografický modul podporují, je dostačující, pokud

a) tyto postupy splňují bezpečnostní požadavky na tyto moduly uvedené ve standardu pro důvěryhodné systémy, který je uveden v bodu 1 přílohy č. 1 této vyhlášky,
b) je modul používán pouze pro označování vydávaných kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, seznamu zneplatněných certifikátů nebo pro označování kvalifikovaných časových razítek,
c) je nasazení a používání modulu v souladu s technickou dokumentací modulu výrobce nebo dodavatele,
d) je modul umístěn a používán v prostorech, které jsou zabezpečeny obdobně jako zabezpečené oblasti kategorie „Důvěrné“ podle zvláštního právního předpisu[1)].

(3) Splnění požadavků stanovených v odstavci 1 písm. a) se dokládá dokladem o provedeném hodnocení a certifikaci bezpečného kryptografického modulu podle požadavků standardu pro tyto moduly, který je uveden v bodu 8 přílohy č. 1 této vyhlášky, nebo podle požadavků standardu pro tyto moduly, který je uveden v bodu 9 přílohy č. 1 této vyhlášky.

(4) Splnění požadavků stanovených v odstavci 1 písm. b) se dokládá dokladem o výsledku hodnocení bezpečného kryptografického modulu podle odstavce 1 písm. b) a dokladem o vyhodnocení shody podle § 9 odst. 2 písm. f) zákona.

(5) Splnění požadavků stanovených v odstavci 2 se dokládá prostřednictvím

a) bezpečnostní dokumentace,
b) podrobného popisu funkcí a technickou dokumentací bezpečného kryptografického modulu v rozsahu nutném pro jeho pořízení.

(6) Pokud doklad podle odstavce 3 nebo odstavce 4 pozbyl platnosti a poskytovatel je schopen zajistit do doby nahrazení kryptografického modulu bezpečným kryptografickým modulem bezpečnost jeho funkcí na stejné úrovni, jakou zajišťoval v době před pozbytím platnosti dokladu, může modul používat za podmínky, že

a) bez zbytečného odkladu uplatní opatření, která přiměřeně eliminují rizika, na základě kterých pozbyly tyto doklady platnosti,
b) v analýze rizik je jako riziko označen stav, kdy doklad podle odstavce 3 nebo odstavce 4 pozbyl platnosti,
c) plán pro zvládání krizových situací stanoví opatření, která poskytovatel uplatní pro zajištění požadované bezpečnosti jeho funkcí,
d) zajistí, aby plnění opatření podle písmene c) bylo kontrolováno tak, aby bylo možné kdykoliv zjistit, že tato opatření nejsou uplatňována nebo nejsou uplatňována v plném rozsahu, a ihned zajistit nápravu,
e) zahájí akvizici bezpečného kryptografického modulu.

§ 21

**Prostředky pro bezpečné vytváření elektronických podpisů**

(1) Poskytovatel zajistí, aby prostředky pro bezpečné vytváření elektronických podpisů, které vydává,

a) splňovaly požadavky na tyto prostředky stanovené standardem pro tyto prostředky, který je uveden v bodu 10 přílohy č. 1 této vyhlášky,
b) měly vyhodnocenou shodu podle § 9 odst. 2 písm. f) zákona,
c) byly poskytovatelem připraveny a předány uživateli v souladu s bezpečnostními a funkčními požadavky standardu pro důvěryhodné systémy, který je uveden v bodu 1 přílohy č. 1 této vyhlášky,
d) byly poskytovatelem připraveny a předány uživateli v souladu s technickou a uživatelskou dokumentací jeho výrobce nebo dodavatele.

(2) Splnění požadavků podle odstavce 1 písm. a), c) a d) se dokládá

a) dokladem o provedeném hodnocení a certifikaci prostředku podle standardu pro prostředky pro bezpečné vytváření elektronických podpisů, který je uveden v bodu 10 přílohy č. 1 této vyhlášky,
b) bezpečnostní dokumentací,
c) podrobným popisem funkcí a technickou a uživatelskou dokumentací vyhodnocovaného prostředku; uživatelská dokumentace musí být v českém jazyce.

## HLAVA DRUHÁ
## Požadavky na ochranu dat pro vytváření elektronických značek

### § 22

(1) Označování daty pro vytváření elektronických značek musí být ihned přerušeno v případě selhání řádné funkce prostředku pro vytváření elektronických značek nebo v případě selhání funkcí aplikace, ve které je používán; v označování se může pokračovat v době, kdy jsou prostředek i aplikace uvedeny do řádného stavu.

(2) Označování daty pro vytváření elektronických značek musí být bezodkladně ukončeno v případě zneužití nebo vzniku důvodné obavy ze zneužití těchto dat.

(3) Označující osoba vytváří a uchovává záznamy o událostech souvisejících s jakýmkoliv nakládáním s prostředky pro vytváření elektronických značek a s daty pro vytváření elektronických značek, která jsou v nich uložena, v průběhu jejich celého životního cyklu.

### § 23

(1) Pokud jsou data pro vytváření elektronických značek používána k označování datových zpráv podle § 11 odst. 2 zákona, mohou být vytvořena, uložena a používána výhradně v kryptografickém prostředku pro vytváření elektronických značek (dále jen „kryptografický prostředek“) a nesmí být používána pro jiný účel, než je vytváření elektronických značek.

(2) Pokud kryptografický prostředek podle odstavce 1 není kryptografickým modulem, který splňuje požadavky stanovené v § 20 odst. 1 této vyhlášky, mohou v něm být uložena výhradně

a) data pro vytváření elektronických značek,
b) data a aplikace nezbytné pro použití dat podle písmena a) při označování datových zpráv a pro přenos dat pro vytváření elektronických značek na jiný kryptografický prostředek.

(3) Kryptografický prostředek podle odstavce 2 může být použit výhradně pro

a) vytvoření a uložení dat a aplikací podle odstavce 2,

b) vytváření elektronických značek.

(4) Pokud je kryptografickým prostředkem kryptografický modul, který splňuje požadavky stanovené v § 20 odst. 1 této vyhlášky, mohou v něm být vytvořena, uložena a používána i jiná data a aplikace, pokud na základě provedené analýzy rizik, při které bylo toto riziko hodnoceno, není takové použití vyloučeno.

(5) Pokud kryptografický prostředek umožňuje přenos dat pro vytváření elektronických značek do jiného kryptografického prostředku, musí být způsob tohoto přenosu důvěryhodný; kryptografický prostředek, na který jsou data přenášena, musí splňovat požadavky odstavců 2 a 3 nebo odstavce 4.

§ 24

(1) Označující osoba, která označuje datové zprávy podle § 11 odst. 2 zákona, dokládá způsob zajištění postupů, které podporují kryptografické prostředky při ochraně dat pro vytváření elektronických značek prostřednictvím interní směrnice, a to vždy

a) pro jakékoliv nakládání s těmito kryptografickými prostředky, a to v průběhu jejich celého životního cyklu, včetně postupů při ukončení jejich používání,
b) pro stanovení oprávnění osob pro jakékoliv nakládání s těmito kryptografickými prostředky,
c) pro zajištění bezpečnosti prostředí, ve kterém jsou používány, včetně zásad při výskytu mimořádné události, která může ohrozit jejich ochranu.

(2) Označující osoba podle odstavce 1 seznamuje osoby, které nakládají s kryptografickými prostředky, s postupy podle odstavce 1 v rozsahu nezbytném k plnění jejich povinností.

(3) Označující osoba průběžně kontroluje správnost postupů podle odstavců 1 a 2 a podle § 22 a 23 a v případě zjištění nedostatků přijímá opatření k jejich odstranění.

## ČÁST TŘETÍ

## ZÁVĚREČNÁ USTANOVENÍ

§ 25

**Přechodná ustanovení**

(1) Poskytovatelé, kteří nejsou akreditováni ministerstvem a kteří zahájili poskytování kvalifikované certifikační služby, a poskytovatelé, kterým byla udělena akreditace pro výkon činnosti akreditovaného poskytovatele do data nabytí účinnosti této vyhlášky, uvedou zajišťování kvalifikovaných certifikačních služeb do souladu s touto vyhláškou do 12 měsíců ode dne vyhlášení této vyhlášky. V tomto období budou poskytovatelé postupovat podle dosavadních právních předpisů.

(2) Pokud poskytovatel poskytuje nejméně jednu kvalifikovanou certifikační službu k datu účinnosti této vyhlášky, zajistí provedení prvního auditu systému řízení bezpečnosti informací do 2 let od data nabytí účinnosti této vyhlášky.

§ 26

**Zrušovací ustanovení**

Zrušuje se vyhláška č. 366/2001 Sb., o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu.

§ 27

**Účinnost**

Tato vyhláška nabývá účinnosti patnáctým dnem po jejím vyhlášení s výjimkou ustanovení § 22 až 24, která nabývají účinnosti prvním dnem třetího kalendářního měsíce následujícího po dni jejího vyhlášení.

Ministryně

**Příloha č. 1 k vyhlášce č. 378/2006**

SEZNAM NOREM A STANDARDŮ

1. CWA 14167-1 – Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements.
2. ČSN ETSI TS 101 456 – Elektronické podpisy a infrastruktury; Požadavky na postupy certifikační autority vydávající kvalifikované certifikáty.
3. ČSN ETSI TS 102 023 – Elektronické podpisy a infrastruktury; Požadavky na postupy autorit časových razítek.
4. ČSN ISO/IEC 17799 – Informační technologie – Soubor postupů pro management bezpečnosti informací.
5. ČSN BS 7799-2 – Systém managementu bezpečnosti informací – Specifikace s návodem pro použití.
6. ČSN ISO/IEC TR 13335 – Informační technologie – Směrnice pro řízení bezpečnosti IT 1-3.
7. ČSN EN ISO 19011 – Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu.
8. CWA 14167-2 – Cryptographic module for CSP signing operations with backup - Protection profile – CMCSOB PP.
9. CWA 14167-4 – Cryptographic module for CSP signing operations – Protection profile – CMCSO PP.
10. CWA 14169 – Secure signature-creation devices “EAL 4+”.
11. FIPS PUB 140-1 - Security Requirements for Cryptographic Modules.
12. FIPS PUB 140-2 - Security Requirements for Cryptographic Modules.

**Příloha č. 2 k vyhlášce č. 378/2006**

STRUKTURA CERTIFIKAČNÍ POLITIKY A CERTIFIKAČNÍ PROVÁDĚCÍ SMĚRNICE

**1. Úvod**
**1.1 Přehled**
**1.2 Název a jednoznačné určení dokumentu**
**1.3 Participující subjekty**
1.3.1 Certifikační autority (dále „CA“)
1.3.2 Registrační autority (dále „RA“)
1.3.3 Držitelé kvalifikovaných certifikátů a podepisující nebo označující osoby, kteří požádali o vydání kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu (dále certifikátu), a kterým byl certifikát vydán
1.3.4 Spoléhající se strany
1.3.5 Jiné participující subjekty
**1.4 Použití certifikátu**
1.4.1 Přípustné použití certifikátu
1.4.2 Omezení použití certifikátu
**1.5 Správa politiky**
1.5.1 Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici
1.5.2 Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici
1.5.3 Subjekt odpovědný za rozhodování o souladu postupů poskytovatele s postupy jiných poskytovatelů certifikačních služeb
1.5.4 Postupy při schvalování souladu podle 1.5.3
**1.6 Přehled použitých pojmů a zkratek**

**2. Odpovědnost za zveřejňování a úložiště informací a dokumentace**
**2.1 Úložiště informací a dokumentace**
**2.2 Zveřejňování informací a dokumentace**
**2.3 Periodicita zveřejňování informací**
**2.4 Řízení přístupu k jednotlivým typům úložišť**

**3. Identifikace a autentizace**
**3.1 Pojmenování**
3.1.1 Typy jmen
3.1.2 Požadavek na významovost jmen
3.1.3 Anonymita a používání pseudonymu
3.1.4 Pravidla pro interpretaci různých forem jmen
3.1.5 Jedinečnost jmen
3.1.6 Obchodní značky
**3.2 Počáteční ověření identity**
3.2.1 Ověřování souladu dat, tj. postup při ověřování, zda má osoba data pro vytváření elektronických podpisů odpovídající datům pro ověřování elektronických podpisů nebo data pro vytváření elektronických značek odpovídající datům pro ověřování elektronických značek
3.2.2 Ověřování identity právnické osoby nebo organizační složky státu
3.2.3 Ověřování identity fyzické osoby
3.2.4 Neověřené informace vztahující se k držiteli certifikátu nebo podepisující či označující osobě
3.2.5 Ověřování specifických práv
3.2.6 Kritéria pro interoperabilitu

**3.3 Identifikace a autentizace při zpracování požadavků na výměnu dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu**
3.3.1 Identifikace a autentizace při rutinní výměně dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek a jim odpovídajících dat ověřování elektronických podpisů nebo dat pro ověřování elektronických značek (dále „párová data“)
3.3.2 Identifikace a autentizace při výměně párových dat po zneplatnění certifikátu
**3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu**

**4. Požadavky na životní cyklus certifikátu**
**4.1 Žádost o vydání certifikátu**
4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu
4.1.2 Registrační proces a odpovědnosti poskytovatele a žadatele
**4.2 Zpracování žádosti o certifikát**
4.2.1 Identifikace a autentizace
4.2.2 Přijetí nebo zamítnutí žádosti o certifikát
4.2.3 Doba zpracování žádosti o certifikát
**4.3 Vydání certifikátu**
4.3.1 Úkony CA v průběhu vydávání certifikátu
4.3.2 Oznámení o vydání certifikátu držiteli certifikátu, podepisující nebo označující osobě
**4.4 Převzetí vydaného certifikátu**
4.4.1 Úkony spojené s převzetím certifikátu
4.4.2 Zveřejňování vydaných certifikátů poskytovatelem
4.4.3 Oznámení o vydání certifikátu jiným subjektům
**4.5 Použití párových dat a certifikátu**
4.5.1 Použití dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek a certifikátu držitelem certifikátu, podepisující nebo označující osobou
4.5.2 Použití dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek a certifikátu spoléhající se stranou
**4.6 Obnovení certifikátu**
4.6.1 Podmínky pro obnovení certifikátu
4.6.2 Subjekty oprávněné požadovat obnovení certifikátu
4.6.3 Zpracování požadavku na obnovení certifikátu
4.6.4 Oznámení o vydání obnoveného certifikátu držiteli certifikátu, podepisující nebo označující osobě
4.6.5 Úkony spojené s převzetím obnoveného certifikátu
4.6.6 Zveřejňování vydaných obnovených certifikátů poskytovatelem
4.6.7 Oznámení o vydání obnoveného certifikátu jiným subjektům
**4.7 Výměna dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu**
4.7.1 Podmínky pro výměnu dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu
4.7.2 Subjekty oprávněné požadovat výměnu dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu
4.7.3 Zpracování požadavku na výměnu dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek
4.7.4 Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických značek podepisující nebo označující osobě
4.7.5 Úkony spojené s převzetím certifikátu s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických značek

4.7.6 Zveřejňování vydaných certifikátů s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických značek
4.7.7 Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických značek jiným subjektům
**4.8 Změna údajů v certifikátu**
4.8.1 Podmínky pro změnu údajů v certifikátu
4.8.2 Subjekty oprávněné požadovat změnu údajů v certifikátu
4.8.3 Zpracování požadavku na změnu údajů v certifikátu
4.8.4 Oznámení o vydání certifikátu se změněnými údaji podepisující nebo označující osobě
4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji
4.8.6 Zveřejňování vydaných certifikátů se změněnými údaji
4.8.7 Oznámení o vydání certifikátu se změněnými údaji jiným subjektům
**4.9 Zneplatnění a pozastavení platnosti certifikátu**
4.9.1 Podmínky pro zneplatnění certifikátu
4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu
4.9.3 Požadavek na zneplatnění certifikátu
4.9.4 Doba odkladu požadavku na zneplatnění certifikátu
4.9.5 Maximální doba, za kterou musí poskytovatel realizovat požadavek na zneplatnění certifikátu
4.9.6 Povinnosti spoléhajících se stran při ověřování, zda nebyl certifikát zneplatněn
4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů
4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů
4.9.9 Možnost ověřování statutu certifikátu on-line (dále „OCSP“)
4.9.10 Požadavky při ověřování statutu certifikátu on-line
4.9.11 Jiné způsoby oznamování zneplatnění certifikátu
4.9.12 Případné odlišnosti postupu zneplatnění v případě kompromitace dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek
4.9.13 Podmínky pro pozastavení platnosti certifikátu
4.9.14 Subjekty oprávněné požadovat pozastavení platnosti certifikátu
4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu
4.9.16 Omezení doby pozastavení platnosti certifikátu
**4.10 Služby související s ověřováním statutu certifikátu**
4.10.1 Funkční charakteristiky
4.10.2 Dostupnost služeb
4.10.3 Další charakteristiky služeb statutu certifikátu
**4.11 Ukončení poskytování služeb pro držitele certifikátu, podepisující nebo označující osobu**
**4.12 Úschova dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek u důvěryhodné třetí strany a jejich obnova**
4.12.1 Politika a postupy při úschově a obnovování dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek
4.12.2 Politika a postupy při zapouzdřování a obnovování šifrovacího klíče pro relaci

**5. Management, provozní a fyzická bezpečnost**
**5.1 Fyzická bezpečnost**
5.1.1 Umístění a konstrukce
5.1.2 Fyzický přístup
5.1.3 Elektřina a klimatizace
5.1.4 Vlivy vody
5.1.5 Protipožární opatření a ochrana

5.1.6 Ukládání médií
5.1.7 Nakládání s odpady
5.1.8 Zálohy mimo budovu
**5.2 Procesní bezpečnost**
5.2.1 Důvěryhodné role
5.2.2 Počet osob požadovaných na zajištění jednotlivých činností
5.2.3 Identifikace a autentizace pro každou roli
5.2.4 Role vyžadující rozdělení povinností
**5.3 Personální bezpečnost**
5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost
5.3.2 Posouzení spolehlivosti osob
5.3.3 Požadavky na přípravu pro výkon role, vstupní školení
5.3.4 Požadavky a periodicita školení
5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi
5.3.6 Postihy za neoprávněné činnosti zaměstnanců
5.3.7 Požadavky na nezávislé zhotovitele (dodavatele)
5.3.8 Dokumentace poskytovaná zaměstnancům
**5.4 Auditní záznamy (logy)**
5.4.1 Typy zaznamenávaných událostí
5.4.2 Periodicita zpracování záznamů
5.4.3 Doba uchování auditních záznamů
5.4.4 Ochrana auditních záznamů
5.4.5 Postupy pro zálohování auditních záznamů
5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)
5.4.7 Postup při oznamování události subjektu, který ji způsobil
5.4.8 Hodnocení zranitelnosti
**5.5 Uchovávání informací a dokumentace**
5.5.1 Typy informací a dokumentace, které se uchovávají
5.5.2 Doba uchování uchovávaných informací a dokumentace
5.5.3 Ochrana úložiště uchovávaných informací a dokumentace
5.5.4 Postupy při zálohování uchovávaných informací a dokumentace
5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace
5.5.6 Systém shromažďování uchovávaných informací a dokumentace (interní nebo externí)
5.5.7 Postupy pro získání a ověření uchovávaných informací a dokumentace
**5.6 Výměna dat pro ověřování elektronických značek v nadřízeném kvalifikovaném systémovém certifikátu poskytovatele**
**5.7 Obnova po havárii nebo kompromitaci**
5.7.1 Postup v případě incidentu a kompromitace
5.7.2 Poškození výpočetních prostředků, softwaru nebo dat
5.7.3 Postup při kompromitaci dat pro vytváření elektronických značek poskytovatele
5.7.4 Schopnost obnovit činnost po havárii
**5.8 Ukončení činnosti CA nebo RA**

**6. Technická bezpečnost**
**6.1 Generování a instalace párových dat**
6.1.1 Generování párových dat
6.1.2 Předání dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek podepisující nebo označující osobě
6.1.3 Předání dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek poskytovateli certifikačních služeb

6.1.4 Poskytování dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek certifikační autoritou spoléhajícím se stranám
6.1.5 Délky párových dat
6.1.6 Generování parametrů dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek a kontrola jejich kvality
6.1.7 Omezení pro použití dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek
**6.2 Ochrana dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek a bezpečnost kryptografických modulů**
6.2.1 Standardy a podmínky používání kryptografických modulů
6.2.2 Sdílení tajemství
6.2.3 Úschova dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek
6.2.4 Zálohování dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek
6.2.5 Uchovávání dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek
6.2.6 Transfer dat pro vytváření elektronických značek do kryptografického modulu nebo z kryptografického modulu
6.2.7 Uložení dat pro vytváření elektronických značek v kryptografickém modulu
6.2.8 Postup při aktivaci dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek
6.2.9 Postup při deaktivaci dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek
6.2.10 Postup při zničení dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek
6.2.11 Hodnocení kryptografických modulů
**6.3 Další aspekty správy párových dat**
6.3.1 Uchovávání dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek
6.3.2 Maximální doba platnosti certifikátu vydaného podepisující nebo označující osobě a párových dat
**6.4 Aktivační data**
6.4.1 Generování a instalace aktivačních dat
6.4.2 Ochrana aktivačních dat
6.4.3 Ostatní aspekty aktivačních dat
**6.5 Počítačová bezpečnost**
6.5.1 Specifické technické požadavky na počítačovou bezpečnost
6.5.2 Hodnocení počítačové bezpečnosti
**6.6 Bezpečnost životního cyklu**
6.6.1 Řízení vývoje systému
6.6.2 Kontroly řízení bezpečnosti
6.6.3 Řízení bezpečnosti životního cyklu
**6.7 Síťová bezpečnost**
**6.8 Časová razítka**

**7. Profily certifikátu, seznamu zneplatněných certifikátů a OCSP**
**7.1 Profil certifikátu**
7.1.1 Číslo verze
7.1.2 Rozšiřující položky v certifikátu