

# Certifikační politika PostSignum Root QCA pro Kvalifikované systémové certifikáty podřízených CA

Verze 2.0

## OBSAH

<b>1 ÚVOD .....</b>	<b>5</b>
1.1 Přehled .....	5
1.2 Název a jednoznačné určení dokumentu .....	5
1.3 Participující subjekty .....	5
1.4 Použití certifikátu .....	7
1.5 Správa politiky .....	8
1.6 Přehled použitých pojmů a zkratk .....	9
<b>2 Odpovědnost za zveřejňování a úložiště informací a dokumentace.....</b>	<b>11</b>
2.1 Úložiště informací a dokumentace.....	11
2.2 Zveřejňování informací a dokumentace.....	11
2.3 Periodicita zveřejňování informací .....	12
2.4 Řízení přístupu k jednotlivým typům úložišť .....	12
<b>3 Identifikace a autentizace .....</b>	<b>12</b>
3.1 Pojmenování.....	12
3.2 Počáteční ověření identity .....	13
3.3 Identifikace a autentizace při zpracování požadavků na výměnu dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu.....	14
3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu.....	14
<b>4 Požadavky na životní cyklus certifikátu.....</b>	<b>14</b>
4.1 Žádost o vydání certifikátu .....	14
4.2 Zpracování žádosti o certifikát.....	16
4.3 Vydání certifikátu .....	16
4.4 Převzetí vydaného certifikátu.....	16
4.5 Použití párových dat a certifikátu .....	17
4.6 Obnovení certifikátu .....	17
4.7 Výměna dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu .....	18
4.8 Změna údajů v certifikátu .....	19
4.9 Zneplatnění a pozastavení platnosti certifikátu.....	19
4.10 Služby související s ověřováním statutu certifikátu.....	22
4.11 Ukončení poskytování služeb pro držitele certifikátu, podepisující nebo označující osobu .....	22
4.12 Úschova dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek u důvěryhodné třetí strany a jejich obnova .....	22
<b>5 Management, provozní a fyzická bezpečnost .....</b>	<b>23</b>
5.1 Fyzická bezpečnost .....	23
5.2 Procesní bezpečnost .....	24
5.3 Personální bezpečnost .....	25
5.4 Auditní záznamy (logy) .....	26
5.5 Uchovávání informací a dokumentace.....	27
5.6 Výměna dat pro ověřování elektronických značek v nadřazeném kvalifikovaném systémovém certifikátu poskytovatele .....	28
5.7 Obnova po havárii nebo kompromitaci.....	29
5.8 Ukončení činnosti CA nebo RA.....	30

<b>6</b>	<b>Technická bezpečnost.....</b>	<b>30</b>
6.1	Generování a instalace párových dat .....	30
6.2	Ochrana dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek a bezpečnost kryptografických modulů .....	32
6.3	Další aspekty správy párových dat.....	33
6.4	Aktivační data .....	34
6.5	Počítačová bezpečnost .....	34
6.6	Bezpečnost životního cyklu .....	35
6.7	Síťová bezpečnost .....	35
6.8	Časová razítka .....	35
<b>7</b>	<b>Profily certifikátu, seznamu zneplatněných certifikátů a OCSP .....</b>	<b>35</b>
7.1	Profil certifikátu .....	35
7.2	Profil seznamu zneplatněných certifikátů .....	38
7.3	Profil OCSP.....	39
<b>8</b>	<b>Hodnocení shody a jiná hodnocení .....</b>	<b>39</b>
8.1	Periodicita hodnocení nebo okolnosti pro provedení hodnocení .....	39
8.2	Identita a kvalifikace hodnotitele .....	39
8.3	Vztah hodnotitele k hodnocenému subjektu .....	39
8.4	Hodnocené oblasti.....	39
8.5	Postup v případě zjištění nedostatků .....	39
8.6	Sdělování výsledků hodnocení.....	40
<b>9</b>	<b>Ostatní obchodní a právní záležitosti .....</b>	<b>40</b>
9.1	Poplatky .....	40
9.2	Finanční odpovědnost .....	40
9.3	Citlivost obchodních informací.....	41
9.4	Ochrana osobních údajů.....	41
9.5	Práva duševního vlastnictví .....	42
9.6	Zastupování a záruky .....	42
9.7	Zřeknutí se záruk.....	43
9.8	Omezení odpovědnosti.....	43
9.9	Odpovědnost za škodu, náhrada škody .....	43
9.10	Doba platnosti, ukončení platnosti.....	43
9.11	Komunikace mezi zúčastněnými subjekty .....	43
9.12	Změny .....	44
9.13	Řešení sporů .....	44
9.14	Rozhodné právo .....	44
9.15	Shoda s právními předpisy .....	45
9.16	Další ustanovení .....	45
9.17	Další opatření .....	45

## Evidence revizí a změn

Verze	Účinnost od	Důvod a popis změny	Autor	Schválil
1.15	5.4.2005	První verze	PCA ČP	PAA ČP
1.17	30.6.2005	Aktualizace dokumentu	PCA ČP	PAA ČP
1.18	30.8.2005	Aktualizace dokumentu	PCA ČP	PAA ČP
1.20	1.9.2006	Aktualizace dokumentu	PCA ČP	PAA ČP
1.21	17.8.2007	Aktualizace dokumentu	PCA ČP	PAA ČP
2.00	13.1.2010	Aktualizace dokumentu	PCA ČP	PAA ČP

## 1 ÚVOD

Tento dokument stanoví pravidla a postupy, podle kterých kořenová certifikační autorita PostSignum Root QCA vydává kvalifikované systémové certifikáty pro ověření elektronické značky certifikační autority. Certifikáty jsou vydávány podřízeným certifikačním autoritám, které jsou provozovány v rámci hierarchie PostSignum České pošty.

### 1.1 Přehled

Česká pošta, s.p. (dále i ČP či Česká pošta) ustavila dvouúrovňovou hierarchii certifikačních autorit s názvem PostSignum. Tato certifikační politika popisuje pravidla, podle kterých vydává certifikáty kořenová certifikační autorita PostSignum Root QCA.

Certifikáty vydané podle této politiky jsou kvalifikované systémové certifikáty ve smyslu zákona o elektronickém podpisu [ZoEP]. Jsou vydávány podřízeným certifikačním autoritám, které jsou provozovány v rámci hierarchie PostSignum České pošty.

Certifikační autorita, které byl vydán certifikát podle této certifikační politiky, musí být provozována Českou poštou, s.p.

Držiteli certifikátů vydaných PostSignum Root QCA jsou tedy certifikační autority provozované Českou poštou, které vydávají certifikáty dalším subjektům, jež však již nejsou certifikačními autoritami.

Soukromý klíč odpovídající veřejnému klíči v certifikátu vydaném autoritou PostSignum Root QCA je určen:

- k podpisu certifikátů subjektů, které nejsou certifikačními autoritami,
- k podpisu seznamu zneplatněných certifikátů (Certificate Revocation List – CRL).

Pravidla pro vydávání a správu kvalifikovaných systémových certifikátů podle této politiky jsou dále popsána v aktuální Certifikační prováděcí směrnici PostSignum QCA, verze 1.30 a vyšší.

### 1.2 Název a jednoznačné určení dokumentu

Tab. 1 Identifikace politiky

Název dokumentu	Certifikační politika PostSignum Root QCA
Verze dokumentu	2.00
Stav	finální
OID poskytovatele certifikačních služeb	2.23.134
OID PostSignum Root QCA	2.23.134.1.4.2.1
OID této politiky	2.23.134.1.4.1.4.200
Datum vydání	13.1.2010
Doba platnosti	Do odvolání nebo do dne ukončení služeb autorit PostSignum QCA.

### 1.3 Participující subjekty

Česká pošta, s. p., jako poskytovatel certifikačních služeb, ustavila hierarchii certifikačních autorit s názvem PostSignum, v jejímž rámci je provozována kořenová certifikační autorita PostSignum Root QCA

a podřízené certifikační autority poskytující různé certifikační služby. Podřízené certifikační autority mohou být řízeny a provozovány pouze Českou poštou, s.p. (s výjimkou registračních autorit).

Identifikační a kontaktní údaje poskytovatele certifikačních služeb jsou:

Česká pošta, s. p.

IČ 47114983, DIČ CZ47114983

Politických vězňů 909/4, 225 99 Praha 1

tel.: 221 132 111, e-mail: info@cpost.cz

Česká pošta, s. p. se stala akreditovaným poskytovatelem certifikačních služeb dne 3.8.2005 na základě akreditace udělené Ministerstvem informatiky ČR.

### 1.3.1 Certifikační autority (dále „CA“)

PostSignum Root QCA tvoří kořen hierarchie certifikačních autorit působících v rámci PostSignum. Jejím úkolem je především vydávat a spravovat certifikáty certifikačních autorit působících v rámci PostSignum. Bezpečnostní opatření, jimiž je PostSignum Root QCA chráněna, jsou přiměřená významu této certifikační autority.

### 1.3.2 Registrační autority (dále „RA“)

Žádosti o vydání certifikátu podle této certifikační politiky jsou předávány manažerovi QCA, který je spolu s příloženými dokumenty (viz odst. 4.1.2) předává k posouzení Komisi pro certifikační politiky (viz odst. 1.3.5.1).

Kontaktní údaje manažera QCA jsou uvedeny v odst. 1.5.2.

### 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

Certifikáty se vydávají pro certifikační autority, jejichž provozovatelem je Česká pošta. Oprávněným žadatelem o certifikát podřízené certifikační autority je manažer dané certifikační autority.

### 1.3.4 Spoléhající se strany

Spoléhající se stranou (uživatel certifikátu) je libovolná fyzická či právnická osoba spoléhající se na certifikát vydaný PostSignum QCA. Spoléhající se strany nevstupují do smluvního vztahu s poskytovatelem certifikačních služeb.

### 1.3.5 Jiné participující subjekty

#### 1.3.5.1 Externí participující subjekty

Na provozu certifikační autority se dále zejména podílí následující subjekty:

TTC Telekomunikace, s.r.o., IČ 41194403

Třebohostická 987/5, 100 00 Praha 10

tel.: 234 054 166, fax: 234 052 990

Uvedený subjekt zajišťuje provoz a správu externí publikační služby.

ICZ, a.s., IČ 25145444

Na Hřebenech II 1718/10, 140 00 Praha 4

tel.: 222 271 111, fax: 222 271 112

Uvedený subjekt je hlavním dodavatelem certifikační autority PostSignum QCA.

### 1.3.5.2 Interní participující subjekty

#### Komise pro certifikační politiky ČP

Komise pro certifikační politiky ČP (Policy Approval Authority – PAA ČP) je orgán, který ustavuje, sleduje a udržuje politiky, jimiž se řídí činnost certifikačních autorit v hierarchii PostSignum. Jedná se jak o politiky pro kořenovou certifikační autoritu (PostSignum Root QCA), tak o politiky pro podřízené certifikační autority (PostSignum Qualified CA).

#### Komise pro certifikační politiky ČP

- ustavuje Tým pro tvorbu certifikačních politik ČP, řídí a kontroluje jeho činnost,
- schvaluje nové certifikační politiky,
- udržuje a kontroluje existující politiky,
- zodpovídá za konzistenci a integritu politik,
- schvaluje veškeré změny certifikačních politik,
- zodpovídá za publikování aktuální verze certifikačních politik.

Komisi pro certifikační politiky ČP je možné kontaktovat na adrese

paa.postsignum@cpost.cz

#### Tým pro tvorbu certifikačních politik ČP

Tým pro tvorbu certifikačních politik České pošty (Policy Creation Authority – PCA ČP) je zodpovědný za tvorbu politik, které předkládá ke schválení Komisi pro politiky ČP. PCA ČP je dle potřeby ustavován Komisí pro certifikační politiky ČP, je jí řízen a kontrolován.

## 1.4 Použití certifikátu

### 1.4.1 Přípustné použití certifikátu

Kvalifikované systémové certifikáty vydané podle této certifikační politiky mohou být použity pouze pro ověření elektronické značky podřízené certifikační autority v hierarchii PostSignum na jí vydaných certifikátech nebo seznamech zneplatněných certifikátů v souladu se zákonem o elektronickém podpisu [ZoEP].

#### 1.4.2 Omezení použití certifikátu

Kvalifikované certifikáty vydávané podle této certifikační politiky je možné využívat pouze v souvislosti s řádnými a legálními účely a v souladu s platnými právními předpisy.

#### 1.5 Správa politiky

Za iniciování změn v certifikační politice nebo inicializaci vytvoření nové certifikační politiky je odpovědný manažer QCA. Ten předá požadavek týmu pro tvorbu certifikačních politik (PCA ČP).

Veškeré změny v této certifikační politice podléhají schválení Komise pro certifikační politiky ČP (PAA ČP). PAA ČP přidělí nové číslo verze, které umožňuje danou verzi identifikovat.

PAA ČP rozhodne, zda nová verze certifikační politiky bude zveřejněna na webových stránkách PostSignum QCA nebo též jinou formou, případně jak.

V případě připravovaných větších změn certifikační politiky, tj. změn, které mají dopad na použitelnost certifikátu, záruky, odpovědnost nebo procesy (a které vyvolá i změnu OID), bude připravovaná změna zveřejněna způsobem uvedeným v odstavci 9.12.2.

##### 1.5.1 Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

Za správu této certifikační politiky je odpovědný poskytovatel certifikačních služeb, tedy Česká pošta, s.p., konkrétně manažer QCA.

##### 1.5.2 Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

Kontaktní osobou ve věci správy této certifikační politiky je manažer QCA. Další informace je možné získat na emailové adrese

[manager.postsignum@cpost.cz](mailto:manager.postsignum@cpost.cz)

nebo na WWW stránkách poskytovatele

<http://qca.postsignum.cz>

##### 1.5.3 Subjekt odpovědný za rozhodování o souladu postupů poskytovatele s postupy jiných poskytovatelů certifikačních služeb

Za správu této certifikační politiky odpovídá manažer QCA, který rovněž rozhoduje o souladu postupů s postupy jiných poskytovatelů certifikačních služeb.

##### 1.5.4 Postupy při schvalování souladu podle 1.5.3

Tento dokument je vytvářen týmem pro tvorbu certifikačních politik ČP (Policy Creation Authority – PCA ČP). PCA ČP je dle potřeby ustavován Komisí pro certifikační politiky ČP, je jí řízen a kontrolován. PCA ČP předává dokument ke schválení Komisi pro certifikační politiky.

Nové verze certifikačních politik a certifikační prováděcí směrnice vznikají podle potřeby, zejména však:

- při takové změně PostSignum QCA (např. změně postupů), která ovlivní obsah těchto dokumentů,



- pokud při pravidelné kontrole okolního prostředí PostSignum QCA byly identifikovány požadavky na změny těchto dokumentů.

Za iniciování změn v certifikační politice nebo v CPS nebo za inicializaci vytvoření nové certifikační politiky nebo CPS je odpovědný manažer QCA. Při přípravě změn v certifikační politice nebo v CPS rozhodne manažer QCA na základě seznamu identifikovaných změn, jakým způsobem budou plánované změny zveřejněny. Komise pro certifikační politiky podle potřeby ustanoví PCA ČP, kterému manažer QCA následně předá seznam požadovaných změn k zapracování. Vypracované politiky nebo CPS předloží manažer QCA ke schválení Komisi pro certifikační politiky, která potom potvrdí OID (pouze politiky) a přidělí číslo verze.

## 1.6 Přehled použitých pojmů a zkratk

**Coordinated Universal Time (UTC)** – Koordinovaný světový čas, časový standard založený na Mezinárodním atomovém čase (TAI).

**CRL (Certificate Revocation List)** – seznam zneplatněných certifikátů. Obsahuje certifikáty, které nadále nelze pokládat za platné například z důvodu prozrazení odpovídajícího soukromého klíče subjektu. CRL je digitálně podepsán vystavitelem certifikátů – certifikační autoritou.

**Držitel certifikátu** – zákazník od okamžiku vydání certifikátu.

**Komise pro certifikační politiky ČP (Policy Approval Authority – PAA)** – orgán, v jehož pravomoci je schvalovat, sledovat a udržovat politiky a CPS, jimiž se řídí činnost certifikační autority.

**Kontaktní místo ČP** – pracoviště České pošty určené pro nabídku vybraných služeb klientům.

**Kvalifikovaný certifikát** – kvalifikovaný certifikát ve smyslu zákona o elektronickém podpisu [ZoEP].

**Kvalifikovaný systémový certifikát** – kvalifikovaný systémový certifikát ve smyslu zákona o elektronickém podpisu [ZoEP].

**Mobilní registrační autorita** – mobilní pracoviště České pošty, jehož základním úkolem je přebírat žádosti o certifikát nebo jeho zneplatnění, kontrolovat identitu žadatelů, poté přijmout nebo zamítnout žádost a předat vydaný certifikát žadateli nebo tento certifikát zneplatnit.

**Následný certifikát** – kvalifikovaný (systémový) certifikát vydaný na základě uzavřené smlouvy jako náhrada za již vydaný certifikát PostSignum Qualified CA; údaje v položce Subject následného certifikátu musí být shodné s údaji v certifikátu, který je nahrazován. Pro vydání následného certifikátu není vyžadována fyzická návštěva registrační autority.

**Obchodní místo** – centrální regionální pracoviště odpovědné za uzavírání a evidenci smluv (někdy také kontaktní místo).

**Pověřená osoba** – ten, kdo vůči certifikační autoritě vystupuje jako zástupce zákazníka – organizace. Pověřené osoby musí být vyjmenovány ve smlouvě mezi zákazníkem a Českou poštou.

**Označující osoba** – osoba definovaná zákonem o elektronickém podpisu [ZoEP].

**Párová data (klíčový pár)** – Jsou základním primitivem asymetrické kryptografie. Tvoří je soukromý a veřejný klíč. Z hlediska důvěrnosti je potřebné chránit především jejich generování a soukromý klíč.

**Podpisující osoba** – osoba definovaná zákonem o elektronickém podpisu [ZoEP].

**PostSignum** – hierarchie certifikačních autorit a autority časového razítka tvořená kořenovou certifikační autoritou PostSignum Root QCA, všemi podřízenými certifikačními autoritami, pro něž PostSignum Root QCA vydala certifikát, a autoritami časového razítka, pro které některá z certifikačních autorit PostSignum vydala kvalifikovaný systémový certifikát.

**PostSignum QCA** – hierarchie certifikačních autorit, vydávajících kvalifikované certifikáty a kvalifikované systémové certifikáty ve smyslu zákona o elektronickém podpisu [ZoEP].

**PostSignum Root QCA** – kořenová certifikační autorita, která má samopodepsaný kvalifikovaný systémový certifikát. Vydává kvalifikované systémové certifikáty pro podřízené certifikační autority a CRL.

**PostSignum Qualified CA** – certifikační autorita, která má kvalifikovaný systémový certifikát podepsaný kořenovou certifikační autoritou PostSignum Root QCA. Vydává kvalifikované certifikáty a kvalifikované systémové certifikáty pro subjekty, které nejsou certifikačními autoritami.

**QCA ČP** – viz PostSignum QCA.

**Registrační autorita** – pracoviště, jehož základním úkolem je přebírat žádosti o certifikát nebo jeho zneplatnění, kontrolovat identitu žadatelů, poté přijmout nebo zamítnout žádost a předat vydaný certifikát žadateli nebo tento certifikát zneplatnit.

**Rozlišovací jméno** – jednoznačně identifikuje podepisující resp. označující osobu dle pravidel definovaných příslušnou certifikační politikou.

**Soukromý klíč** – souhrnné označení dat pro vytváření elektronického podpisu a dat pro vytváření elektronických značek

**Správa žadatelů** – aplikace QCA zajišťující informační podporu procesu registrace a evidence (dále také SŽ).

**Tým pro tvorbu certifikačních politik (Policy Creation Authority – PCA)** – tým, který vytváří politiky, jež předkládá ke schválení Komisi pro certifikační politiky. PCA je ustaven Komisí pro certifikační politiky, která řídí a kontroluje jeho činnost.

**Uživatel certifikátu (relying party)** – osoba, která užívá certifikát vydaný PostSignum Root QCA například pro ověření digitálního podpisu či značky nebo pro zajištění jiných bezpečnostních služeb. Jinak též označována jako Osoba spoléhající se na certifikát.

**Veřejný klíč** – souhrnné označení dat pro ověřování elektronického podpisu nebo dat pro ověřování elektronických značek

**Zákazník** – fyzická či právnická osoba, která uzavírá s Českou poštou smlouvu o poskytování certifikačních služeb. PostSignum QCA rozlišuje dva typy zákazníků: zákazník – organizace a zákazník – fyzická osoba.

**Zákazník – organizace** – subjekt, který požaduje uvedení jména organizace a identifikačního čísla v certifikátu.

**Zákazník – fyzická osoba** – nepodnikající osoba, nebo podnikající osoba bez přiřazeného identifikačního čísla.

**Žadatel** – osoba, která má právo žádat u PostSignum Root QCA o certifikát podle některé z platných certifikačních politik; jedná se mj. o souhrnné označení pro podepisující a označující osobu.

## 2 ODPOVĚDNOST ZA ZVEŘEJŇOVÁNÍ A ÚLOŽIŠTĚ INFORMACÍ A DOKUMENTACE

### 2.1 Úložiště informací a dokumentace

Jednotlivá úložiště informací a dokumentace provozuje a za jejich provoz odpovídá Česká pošta, s. p. jako poskytovatel certifikačních služeb.

Jedinou výjimkou je úložiště na adrese postsignum.ttc.cz provozované společností TTC Telekomunikace, s.r.o na základě smlouvy s Českou poštou, s. p.

Za zveřejňování informací odpovídá Česká pošta, s. p. jako poskytovatel certifikačních služeb.

### 2.2 Zveřejňování informací a dokumentace

Vydané certifikáty jsou uloženy v databázi certifikační autority.

Informace o vydaných certifikátech, o provozu PostSignum QCA a dokumentace PostSignum QCA jsou zveřejňovány v níže uvedeném rozsahu.

#### 2.2.1 Zveřejňování certifikátů a CRL

Certifikáty certifikačních autorit a vydané certifikáty jsou zveřejňovány

- na webových stránkách PostSignum QCA  
<http://www.postsignum.cz>, nebo
- na registračních autoritách, kde je možné požádat o jejich zkopírování na přinesené médium.

Informace o stavu certifikátu jsou zveřejňovány ve formě seznamu zneplatněných certifikátů (CRL)

- na webových stránkách PostSignum QCA

<http://www.postsignum.cz>

<http://www2.postsignum.cz>

<http://postsignum.ttc.cz>

#### 2.2.2 Zveřejňování informací o certifikační autoritě

Zpráva pro uživatele a případně i certifikační politiky nebo další dokumenty jsou zveřejňovány na

- webových stránkách PostSignum QCA

<http://www.postsignum.cz>

Další důležité informace, zejména informace požadované zákonem [ZoEP] nebo vyhláškou [V378] (např. odnětí akreditace, zneplatnění systémového certifikátu certifikační autority) nebo informace o mimořádné události jsou zveřejňovány

- na webových stránkách PostSignum QCA,

<http://www.postsignum.cz>

- v celostátně distribuovaném deníku (konkrétně deníku Hospodářské noviny).

### 2.3 Periodicita zveřejňování informací

Informace jsou zveřejňovány v následujících intervalech:

- certifikační politiky, certifikační prováděcí směrnice a zpráva pro uživatele jsou zveřejňovány (pokud jsou určeny ke zveřejnění) po schválení a vydání nové verze, vždy však před počátkem platnosti daného dokumentu (a v případě certifikační politiky před vydáním prvního certifikátu);
- certifikáty, pokud byly označeny pro zveřejnění, jsou zveřejňovány elektronickou cestou nejpozději do 24 hodin od převzetí certifikátu držitelem;
- informace o stavu certifikátu ve formě seznamu zneplatněných certifikátů (CRL) jsou zveřejňovány neprodleně po jejich vydání, nejpozději před koncem platnosti posledního zveřejněného seznamu zneplatněných certifikátů (tj. alespoň jednou za 12 měsíců) a
- důležité informace, zejména informace požadované [ZoEP] nebo [V378] jsou zveřejňovány neprodleně.

### 2.4 Řízení přístupu k jednotlivým typům úložišť

Certifikační politiky (pokud jsou určeny ke zveřejnění), certifikáty certifikačních autorit a seznamy zneplatněných certifikátů a další důležité informace jsou přístupné pro čtení bez jakéhokoliv omezení.

Modifikace zveřejněných údajů je povolena pouze autorizované obsluze a procesům certifikační autority.

## 3 IDENTIFIKACE A AUTENTIZACE

### 3.1 Pojmenování

#### 3.1.1 Typy jmen

Jméno subjektu je konstruováno podle standardu X.501 resp. návazného standardu X.520.

#### 3.1.2 Požadavek na významovost jmen

Význam údajů použitých v attributech subjektu certifikátu a v rozšířeních certifikátu je popsán v kapitole 7.

#### 3.1.3 Anonymita a používání pseudonymu

Česká pošta nepodporuje pseudonym v položce Subject certifikátu podřízené certifikační autority.

#### 3.1.4 Pravidla pro interpretaci různých forem jmen

V certifikátech vydávaných PostSignum Root CA jsou podporovány pouze následující znakové sady:

- UTF8, znaky středoevropské znakové sady,
- US ASCII.

Veškeré údaje dokladované při registraci žádosti o certifikát podřízené CA se do žádostí o certifikáty a do certifikátů vydávaných PostSignum Root QCA přenášejí ve tvaru, ve kterém jsou uvedeny v předkládaných dokladech. Transkripce, jako například odstranění diakritiky, není možná.

### 3.1.5 Jedinečnost jmen

PostSignum Root QCA si vyhrazuje právo upravit označení držitele certifikátu (položka Subject v certifikátu) tak, aby byla zaručena jednoznačnost jména, tedy aby stejné rozlišovací jméno nebylo přiřazeno dvěma různým subjektům.

### 3.1.6 Obchodní značky

Všechna pole certifikátu vydaného podle této politiky, musí obsahovat údaje vztahující se k příslušné podřízené certifikační autoritě. Certifikát může obsahovat pouze obchodní značky nebo registrované obchodní známky, které jsou vlastněné Českou poštou, s. p., nebo ke kterým má příslušný souhlas vlastníka.

## 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

Žadatel o certifikát předkládá elektronickou žádost ve formátu PKCS#10 obsahující veřejný klíč, která je podepsána soukromým klíčem odpovídajícím veřejnému klíči uvedenému v žádosti. Tím je prokázáno, že žadatel o certifikát v době vytváření žádosti vlastnil soukromý klíč odpovídající veřejnému klíči uvedenému v žádosti.

### 3.2.2 Ověřování identity právnické osoby nebo organizační složky státu

Certifikáty jsou vydávány pro certifikační autority, jejichž provozovatelem je Česká pošta. Oprávněným žadatelem o certifikát podřízené certifikační autority je manažer dané certifikační autority. Svou totožnost a své oprávnění dokládá podle vnitřních předpisů České pošty.

### 3.2.3 Ověřování identity fyzické osoby

Viz ustanovení odst. 3.2.2.

### 3.2.4 Neověřené informace vztahující se k držiteli certifikátu nebo podepisující či označující osobě

Všechny informace uvedené ve vydaném kvalifikovaném systémovém certifikátu podřízené certifikační autority jsou náležitým způsobem ověřené.

### 3.2.5 Ověřování specifických práv

Žádná ustanovení v tomto odstavci.

### 3.2.6 Kritéria pro interoperabilitu

Případná spolupráce s jinými poskytovateli certifikačních služeb je možná až po schválení Komisí pro certifikační politiky ČP, na základě uzavřené smlouvy a za podmínek definovaných toto komisí.

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“)

Platí ustanovení platná pro počáteční ověření identity uvedená v odst. 3.2.

3.3.2 Identifikace a autentizace při výměně párových dat po zneplatnění certifikátu

Platí ustanovení platná pro počáteční ověření identity uvedená v odst. 3.2.

3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu

Oprávněným žadatelem o zneplatnění certifikátu podřízené CA je manažer této CA. Svou totožnost a své oprávnění dokládá podle vnitřních předpisů České pošty.

Ke zneplatnění certifikátu podřízené CA může dojít i z vůle poskytovatele certifikačních služeb. V tomto případě je oprávněným žadatelem o zneplatnění certifikátu manažer QCA.

O zneplatnění certifikátu vydaného jako kvalifikovaný může, jakožto o předběžné opatření, požádat orgán definovaný zákonem o elektronickém podpisu. Oprávněným žadatelem o zneplatnění kvalifikovaného certifikátu je v tomto případě zástupce tohoto orgánu.

## 4 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

4.1 Žádost o vydání certifikátu

4.1.1 Subjekty oprávněně podat žádost o vydání certifikátu

Certifikáty jsou vydávány pro certifikační autority, jejichž provozovatelem je Česká pošta. Oprávněným žadatelem o certifikát podřízené certifikační autority je manažer dané certifikační autority.

4.1.2 Registrační proces a odpovědnosti poskytovatele a žadatele

Písemná žádost o vydání certifikátu podřízené certifikační autority je předkládána Komisi pro certifikační politiky ČP. Žádost musí obsahovat následující identifikační údaje certifikační autority, pro kterou má být vydán certifikát:

- jméno certifikační autority,
- provozovatel certifikační autority – upřesnění provozovatele v rámci České pošty,
- seznam dokumentů přiložených k této žádosti včetně označení verzí těchto dokumentů.

Žádost musí být podepsána zástupcem CA oprávněným k podání žádosti.

K žádosti musí být přiloženy tyto dokumenty:

- certifikační politiky certifikační autority, pro niž má být vydán certifikát,
- certifikační prováděcí směrnice,

- systémová bezpečnostní politika,
- plán zvládnání krizových situací a plán obnovy.

Písemné žádosti a veškeré přiložené doklady jsou archivovány po dobu 5 let od ukončení platnosti certifikátu, minimálně však 10 let.

#### 4.1.2.1 Odpovědnost žadatele

Žadatel je povinen zejména:

- poskytovat pravdivé a úplné informace při registraci žádosti o certifikát
- zkontrolovat, zda údaje uvedené v certifikátu jsou správné a odpovídají požadovaným údajům,
- nakládat se soukromým klíčem, který odpovídá veřejnému klíči v certifikátu vydaném podle této certifikační politiky, s náležitou péčí, a to tak, aby nemohlo dojít k jeho neoprávněnému použití,
- užívat soukromý klíč a odpovídající certifikát vydaný podle této certifikační politiky pouze pro účely stanovené v této certifikační politice,
- neprodleně uvědomit poskytovatele certifikačních služeb o skutečnostech, které vedou ke zneplatnění certifikátu, zejména o podezření, že soukromý klíč byl zneužit, požádat o revokaci certifikátu a ukončit používání příslušného soukromého klíče,
- seznámit se s certifikační politikou, podle které mu byl vydán certifikát.

#### 4.1.2.2 Odpovědnost poskytovatele

Poskytovatel certifikačních služeb je zejména povinen:

- v procesu registrace žadatele o certifikát ověřit všechny údaje podle předložených dokladů,
- vydat certifikát obsahující věcně správné údaje na základě informací, které jsou certifikační autoritě k dispozici v době vydávání certifikátu,
- zveřejňovat certifikační politiky, podle kterých vydává certifikáty, předepsanými způsoby (viz odstavec 2.2),
- zveřejnit kvalifikovaný systémový certifikát poskytovatele certifikačních služeb tak, aby se každý mohl ujistit o jeho identitě,
- věnovat náležitou péči všem činnostem spojeným s poskytováním certifikačních služeb; náležitá péče zahrnuje provoz v souladu
- s platnými právními předpisy,
- s touto certifikační politikou,
- s certifikační prováděcí směrnicí,
- se systémovou bezpečnostní politikou,
- s provozní dokumentací.

## 4.2 Zpracování žádosti o certifikát

### 4.2.1 Identifikace a autentizace

Platí ustanovení odstavce 3.2.2.

### 4.2.2 Přijetí nebo zamítnutí žádosti o certifikát

Komise pro certifikační politiky ČP na základě předložené žádosti rozhodne, zda bude pro danou certifikační autoritu vydán certifikát.

### 4.2.3 Doba zpracování žádosti o certifikát

Rozhodnutí o přijetí nebo zamítnutí žádosti je žadateli o certifikát sděleno do třiceti pracovních dní od podání žádosti.

## 4.3 Vydání certifikátu

### 4.3.1 Úkony CA v průběhu vydávání certifikátu

Po schválení písemné žádosti předá zástupce podřízené certifikační autority manažerovi QCA elektronickou žádost o certifikát ve formátu PKCS#10, obsahující relevantní údaje se stejnými hodnotami, jaké jsou uvedeny v předaných dokumentech. Spolu s elektronickou žádostí o certifikát předává zástupce podřízené CA manažerovi QCA druhou písemnou žádost obsahující následující údaje:

- jméno certifikační autority,
- provozovatel certifikační autority – upřesnění provozovatele v rámci České pošty,
- opis veřejného klíče certifikační autority.

Všechny uvedené údaje musí souhlasit s údaji uvedenými ve schválené písemné žádosti o certifikát. Pokud údaje souhlasí, je do deseti pracovních dnů od okamžiku podání této žádosti vydán certifikát.

Certifikát se stává platným okamžikem vydání.

### 4.3.2 Oznámení o vydání certifikátu držiteli certifikátu, podepisující nebo označující osobě

Poskytovatel certifikačních služeb informuje žadatele o certifikát o vydání certifikátu nejpozději do jednoho pracovního dne od vydání certifikátu.

## 4.4 Převzetí vydaného certifikátu

### 4.4.1 Úkony spojené s převzetím certifikátu

Certifikát podřízené CA je žadateli o certifikát předán ve formátu DER spolu s certifikátem PostSignum Root QCA. Žadatel o certifikát nebo jeho zplnomocněný zástupce osobně přebírá certifikát a kontroluje, zda jsou údaje uvedené v certifikátu v pořádku. Pokud údaje souhlasí, žadatel přebírá certifikát a tento úkon stvrzuje svým podpisem pod protokolem o převzetí certifikátu. Pokud údaje nesouhlasí, poskytovatel certifikačních služeb musí do deseti pracovních dní vydat certifikát s opravenými údaji.

Podpisem protokolu o převzetí certifikátu držitel stvrzuje:

- že na sebe bere závazky vyplývající z certifikační politiky, podle které byl certifikát vydán,



- že mu nejsou známy žádné skutečnosti, které by svědčily o tom, že soukromý klíč odpovídající veřejnému klíči v certifikátu vlastní jiná osoba, než je povoleno v příslušné certifikační politice,
- že údaje ve vydaném certifikátu jsou správné a úplné.

#### 4.4.2 Zveřejňování vydaných certifikátů poskytovatelem

Certifikáty vydané PostSignum Root QCA a určené ke zveřejnění jsou zveřejňovány elektronickou cestou.

#### 4.4.3 Oznámení o vydání certifikátu jiným subjektům

Kromě zveřejnění vydaného certifikátu neoznamuje poskytovatel certifikačních služeb vydání certifikátu žádné třetí straně.

#### 4.5 Použití párových dat a certifikátu

Páry klíčů svázané s certifikáty mají stejnou dobu platnosti jako certifikáty. Klíčové páry, na základě kterých již byl vydán certifikát certifikační autoritou PostSignum Root QCA, nemohou být v prostředí PostSignum Root QCA znovu použity.

##### 4.5.1 Použití dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek a certifikátu držitelem certifikátu, podepisující nebo označující osobou

Označující osoba je povinna zejména:

- nakládat se soukromým klíčem, který odpovídá veřejnému klíči v certifikátu vydaném podle této certifikační politiky, s náležitou péčí, a to tak, aby nemohlo dojít k jeho neoprávněnému použití,
- v případě ztráty, odcizení nebo podezření na kompromitaci soukromého klíče neprodleně o této skutečnosti informovat poskytovatele certifikačních služeb a zároveň ukončit používání uvedeného soukromého klíče,
- užívat soukromý klíč a odpovídající certifikát vydaný podle této certifikační politiky pouze pro účely stanovené v této certifikační politice, uvedené v odst. 1.4.

##### 4.5.2 Použití dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek a certifikátu spoléhající se stranou

Uživatel certifikátu vydaného PostSignum Root QCA (spoléhající se strana) je povinen zejména:

- Získat certifikát PostSignum Root QCA z bezpečného zdroje (webové stránky PostSignum QCA, webové stránky orgánu definovaného zákonem o elektronickém podpisu, na pracovišti registrační autority) a ověřit otisk ("fingerprint") tohoto certifikátu.
- Před použitím certifikátu vydaného PostSignum Root QCA ověřit platnost certifikátu PostSignum Root QCA a následně i platnost vydaného certifikátu; kontrola se provádí na správnost podpisu vydávající autority a vůči příslušnému aktuálnímu CRL a aktuálnímu času.

#### 4.6 Obnovení certifikátu

Obnova certifikátu vydaného podle této certifikační politiky není možná. V odpovídajícím časovém předstihu před vypršením platnosti stávajícího certifikátu požádá žadatel o vydání nového certifikátu (odst. 4.1); není nutné měnit subject certifikátu žadatele.

#### 4.6.1 Podmínky pro obnovení certifikátu

Viz ustanovení odst. 4.6.

#### 4.6.2 Subjekty oprávněné požadovat obnovení certifikátu

Viz ustanovení odst. 4.6.

#### 4.6.3 Zpracování požadavku na obnovení certifikátu

Viz ustanovení odst. 4.6.

#### 4.6.4 Oznámení o vydání obnoveného certifikátu držiteli certifikátu, podepisující nebo označující osobě

Viz ustanovení odst. 4.6.

#### 4.6.5 Úkony spojené s převzetím obnoveného certifikátu

Viz ustanovení odst. 4.6.

#### 4.6.6 Zveřejňování vydaných obnovených certifikátů poskytovatelem

Viz ustanovení odst. 4.6.

#### 4.6.7 Oznámení o vydání obnoveného certifikátu jiným subjektům

Viz ustanovení odst. 4.6.

#### 4.7 Výměna dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu

Při výměně dat pro ověřování elektronických značek v certifikátu je nutné požádat o vydání nového certifikátu (odst. 4.1); není nutné měnit subject certifikátu podřízené certifikační autority.

##### 4.7.1 Podmínky pro výměnu dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu

Viz ustanovení odst. 4.7.

##### 4.7.2 Subjekty oprávněné požadovat výměnu dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu

Viz ustanovení odst. 4.7.

##### 4.7.3 Zpracování požadavku na výměnu dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek

Viz ustanovení odst. 4.7.

##### 4.7.4 Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických značek podepisující nebo označující osobě

Viz ustanovení odst. 4.7.

4.7.5 Úkony spojené s převzetím certifikátu s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických značek

Viz ustanovení odst. 4.7.

4.7.6 Zveřejňování vydaných certifikátů s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických značek

Viz ustanovení odst. 4.7.

4.7.7 Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických značek jiným subjektům

Viz ustanovení odst. 4.7.

4.8 Změna údajů v certifikátu

Certifikát se změněnými údaji lze vydat pouze jako nový certifikát podle postupů uvedených v odstavcích 4.1 - 4.4.

4.8.1 Podmínky pro změnu údajů v certifikátu

Viz ustanovení odstavců uvedených v odstavci 4.8.

4.8.2 Subjekty oprávněné požadovat změnu údajů v certifikátu

Viz ustanovení odstavců uvedených v odstavci 4.8.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

Viz ustanovení odstavců uvedených v odstavci 4.8.

4.8.4 Oznámení o vydání certifikátu se změněnými údaji podepisující nebo označující osobě

Viz ustanovení odstavců uvedených v odstavci 4.8.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Viz ustanovení odstavců uvedených v odstavci 4.8.

4.8.6 Zveřejňování vydaných certifikátů se změněnými údaji

Viz ustanovení odstavců uvedených v odstavci 4.8.

4.8.7 Oznámení o vydání certifikátu se změněnými údaji jiným subjektům

Viz ustanovení odstavců uvedených v odstavci 4.8.

4.9 Zneplatnění a pozastavení platnosti certifikátu

Platnost certifikátu je ukončena v okamžiku jeho zneplatnění a zveřejnění na seznamu zneplatněných certifikátů.

Pokud není certifikát po dobu jeho platnosti nutné zneplatnit, skončí jeho platnost v časovém okamžiku uvedeném v certifikátu. Každý vydaný certifikát zůstává po ukončení své platnosti nadále uložen v

databázi vydávající certifikační autority a archivován v souladu s platnou legislativou a archivačními předpisy České pošty.

#### 4.9.1 Podmínky pro zneplatnění certifikátu

Certifikát může být zneplatněn z vůle držitele certifikátu, z vůle poskytovatele certifikačních služeb nebo na základně nařízení předběžného opatření orgánu definovaného zákonem o elektronickém podpisu.

#### 4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

O zneplatnění certifikátu může požádat držitel certifikátu prostřednictvím manažera podřízené CA, manažer QCA nebo zástupce orgánu definovaného zákonem o elektronickém podpisu.

#### 4.9.3 Požadavek na zneplatnění certifikátu

##### 4.9.3.1 Zneplatnění certifikátu na žádost držitele certifikátu

Manažer podřízené certifikační autority žádá o zneplatnění certifikátu písemně. V žádosti o zneplatnění musí být uveden důvod zneplatnění.

##### 4.9.3.2 Zneplatnění certifikátu z vůle PostSignum Root QCA

Poskytovatel certifikačních služeb může zneplatnit certifikát držitele, který provozuje podřízenou certifikační autoritu v rozporu s dokumenty, jež byly přiloženy k žádosti o certifikát. Důvodem zneplatnění může být rovněž nedodržování pravidel této certifikační politiky nebo podezření na kompromitaci klíče podřízené CA.

Manažer QCA podává písemnou žádost o zneplatnění certifikátu podřízené CA, kterou předá některému z operátorů oprávněných provádět zneplatnění certifikátu. Po úspěšném zneplatnění certifikátu podřízené CA je vytvořen protokol o zneplatnění certifikátu, který je neprodleně zaslán manažerovi podřízené CA. Manažer podřízené CA je o zneplatnění certifikátu podřízené CA informován rovněž telefonicky nebo prostřednictvím elektronické pošty.

##### 4.9.3.3 Zneplatnění certifikátu z vůle orgánu definovaného zákonem o elektronickém podpisu

O zneplatnění certifikátu vydaného jako kvalifikovaný systémový může, jakožto o předběžné opatření, požádat i orgán definovaný zákonem o elektronickém podpisu. Zástupce orgánu definovaného zákonem o elektronickém podpisu žádá o zneplatnění kvalifikovaného certifikátu písemně, v žádosti musí být uveden důvod zneplatnění certifikátu.

Po úspěšném zneplatnění certifikátu podřízené CA je vytvořen protokol o zneplatnění certifikátu, který je neprodleně zaslán manažerovi podřízené CA. Manažer podřízené CA je o zneplatnění certifikátu podřízené CA informován rovněž telefonicky nebo prostřednictvím elektronické pošty.

#### 4.9.4 Doba odkladu požadavku na zneplatnění certifikátu

V okamžiku, kdy se osoba oprávněná žádat o zneplatnění certifikátu dozví skutečnost, která je důvodem pro zneplatnění certifikátu, musí neprodleně požádat o zneplatnění certifikátu.

#### 4.9.5 Maximální doba, za kterou musí poskytovatel realizovat požadavek na zneplatnění certifikátu

Certifikát vydaný podle této certifikační politiky bude zneplatněn neprodleně po přijetí oprávněné žádosti o zneplatnění.

CRL obsahující zneplatněný certifikát vydaný podle této certifikační politiky je zveřejněn neprodleně po zneplatnění certifikátu.

#### 4.9.6 Povinnosti spoléhajících se stran při ověřování, zda nebyl certifikát zneplatněn

Uživatel certifikátu vydaného PostSignum Root QCA (spoléhající se strana) je povinen postupovat v souladu s ustanoveními odst. 4.5.2.

#### 4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů (CRL) PostSignum Root QCA je vydáván a zveřejňován alespoň každých 12 měsíců:

- na webových stránkách PostSignum QCA,
- u nezávislého poskytovatele webových služeb.

Primárním zdrojem aktuálního CRL jsou webové stránky PostSignum QCA.

#### 4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů je zveřejněn co nejdříve po vydání; vždy je dodrženo ustanovení odst. 4.9.5.

#### 4.9.9 Možnost ověřování statutu certifikátu on-line (dále „OCSP“)

PostSignum Root QCA neposkytuje informace o stavu certifikátu protokolem OCSP.

Stav certifikátu je možné ověřit pouze na aktuálním CRL.

#### 4.9.10 Požadavky při ověřování statutu certifikátu on-line

PostSignum QCA tuto službu neposkytuje.

Stav certifikátu je možné ověřit pouze na aktuálním CRL.

#### 4.9.11 Jiné způsoby oznamování zneplatnění certifikátu

Poskytovatel certifikačních služeb neposkytuje žádné další možnosti, kromě výše uvedených, pro ověření stavu certifikátu.

#### 4.9.12 Případné odlišnosti postupu zneplatnění v případě kompromitace dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Postup pro zneplatnění certifikátu v případě kompromitace dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek je shodný s obecným postupem pro zneplatnění certifikátu.

#### 4.9.13 Podmínky pro pozastavení platnosti certifikátu

PostSignum QCA tuto službu neposkytuje.

#### 4.9.14 Subjekty oprávněné požadovat pozastavení platnosti certifikátu

PostSignum QCA tuto službu neposkytuje.

#### 4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu

PostSignum QCA tuto službu neposkytuje.

#### 4.9.16 Omezení doby pozastavení platnosti certifikátu

PostSignum QCA tuto službu neposkytuje.

#### 4.10 Služby související s ověřováním statutu certifikátu

Status certifikátu je možné ověřit na seznamu zneplatněných certifikátů (CRL) v rámci služby umožňující přístup k veřejným informacím PostSignum QCA protokolem HTTP.

##### 4.10.1 Funkční charakteristiky

Seznam zneplatněných certifikátů a informace o stavu certifikátu jsou považovány za veřejně přístupné informace. Seznam zneplatněných certifikátů (CRL) je zveřejňován:

- na webových stránkách PostSignum QCA,
- u nezávislého poskytovatele webových služeb.

Primárním zdrojem aktuálního CRL jsou webové stránky PostSignum QCA.

##### 4.10.2 Dostupnost služeb

Seznam zneplatněných certifikátů je prostřednictvím služby umožňující přístup k veřejným informacím dostupný 7 dní v týdnu 24 hodin denně. Architektura řešení a havarijní plány jsou navrženy tak, aby vždy existovalo alespoň jedno místo, kde je možné získat aktuální Seznam zneplatněných certifikátů.

##### 4.10.3 Další charakteristiky služeb statutu certifikátu

Další charakteristiky služeb statutu certifikátu nejsou stanoveny.

#### 4.11 Ukončení poskytování služeb pro držitele certifikátu, podepisující nebo označující osobu

Poskytování služeb pro držitele certifikátu nebo označující osobu (vzhledem ke skutečnosti, že certifikát je vydán podřízené CA ve správě ČP) je ukončeno okamžikem ukončení poskytování služeb podřízené CA.

#### 4.12 Úschova dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek u důvěryhodné třetí strany a jejich obnova

PostSignum QCA tuto službu neposkytuje.

##### 4.12.1 Politika a postupy při úschově a obnovování dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

PostSignum QCA tuto službu neposkytuje.

##### 4.12.2 Politika a postupy při zapouzdřování a obnovování šifrovacího klíče pro relaci

PostSignum QCA tuto službu neposkytuje.

## 5 MANAGEMENT, PROVOZNÍ A FYZICKÁ BEZPEČNOST

Pro PostSignum QCA byly zpracovány dokumenty:

- Systémová bezpečnostní politika, popisující zásady bezpečnosti v oblasti fyzické, procedurální a personální;
- Plán pro zvládnání krizových situací a plán obnovy, popisující postupy pro zachování garantované úrovně služeb v případě výskytu mimořádné situace,
- Provozní a bezpečnostní procedury, popisující na logické úrovni postupy dodržované v PostSignum QCA, a směrnice
- Organizační zajištění úlohy Kvalifikovaná certifikační autorita České pošty, s. p., která mj. upravuje oblast obsazování rolí PostSignum QCA.

Zmíněné dokumenty byly vypracovány na základě výsledků provedené analýzy rizik.

Tyto dokumenty jsou mj. přístupné osobám, které provádějí kontrolu bezpečnostní shody PostSignum QCA. Tato kapitola vychází z výše uvedených dokumentů a poskytuje stručný přehled základních bezpečnostních zásad uplatňovaných v PostSignum QCA.

### 5.1 Fyzická bezpečnost

Činnosti spojené se správou a provozem PostSignum Root QCA jsou prováděny výhradně na centrálních pracovištích.

#### 5.1.1 Umístění a konstrukce

V PostSignum QCA existují následující typy stabilních pracovišť umístěných v prostorách České pošty, s. p. nebo jejích smluvních partnerů:

- centrální pracoviště (hlavní a záložní lokalita),
- operátorská pracoviště centra (zejména pro správu podpůrného informačního systému),
- pracoviště registrační autority (typicky na kontaktním místě) a
- obchodní místa.

Použitá konstrukce vyplývá z bezpečnostních požadavků uvedených v dokumentu Systémová bezpečnostní politika; obecně platí, že všechny výše uvedené typy pracovišť mají jasně definovaný perimetr a jsou proti neoprávněnému vniknutí chráněny mechanickými prostředky. Centrální pracoviště jsou zabezpečena obdobně jako zabezpečené oblasti kategorie „Důvěrné“.

#### 5.1.2 Fyzický přístup

Pro každý typ pracoviště je v jeho provozním řádu definováno, kteří pracovníci mají na pracoviště fyzický přístup. Prostory jsou chráněny proti neoprávněnému vniknutí mechanickými prostředky (bezpečnostní zámky a mříže), na centrálním pracovišti též samostatnou smyčkou elektronického zabezpečovacího zařízení.

### 5.1.3 Elektřina a klimatizace

Centrální pracoviště jsou připojena na nepřerušitelný zdroj napájení (UPS) a mají nainstalovanou klimatizaci, která udržuje teplotu a vlhkost optimální pro provozovaná zařízení.

### 5.1.4 Vlivy vody

Centrální pracoviště jsou umístěna mimo zátopové oblasti.

Prostory centrálních pracovišť jsou vybaveny signalizací zatopení vodou. Tato signalizace je vyvedena na pracoviště obsazené nepřetržitě 24 hodin denně, 7 dní v týdnu.

### 5.1.5 Protipožární opatření a ochrana

Prostory centrálních pracovišť jsou vybaveny elektronickou požární signalizací (EPS). Tato signalizace je vyvedena na pracoviště obsazené nepřetržitě 24 hodin denně, 7 dní v týdnu.

### 5.1.6 Ukládání médií

Pro účely uskladnění dat PostSignum QCA jsou k dispozici trezory, minimálně jeden z nich je mimo areály budov centrálních pracovišť.

### 5.1.7 Nakládání s odpady

Papírové dokumenty a média, která jsou používána v PostSignum QCA, jsou poté, co nejsou zapotřebí, likvidována bezpečným způsobem:

- média jsou fyzicky zlikvidována nebo je použit vhodný program zajišťující úplné smazání média,
- papírové dokumenty jsou zlikvidovány v zařízení k tomu určeném.

### 5.1.8 Zálohy mimo budovu

Pro PostSignum QCA byla vybudována záložní lokalita, kam provoz přechází v mimořádných situacích, kdy není možné zabezpečit řádný provoz QCA v hlavní lokalitě, a kam jsou také pravidelně zasílány zálohy systémů PostSignum QCA.

## 5.2 Procesní bezpečnost

### 5.2.1 Důvěryhodné role

V PostSignum QCA byly definovány role, které zastává obsluha PostSignum QCA. Jsou stanovena pravidla, podle kterých jsou role obsazovány, tedy kdo pracovníka v dané roli jmenuje a odvolává, které role nesmí zastávat současně jedna osoba. Veškerá přístupová práva (na úrovni fyzického přístupu, na úrovni přístupu k operačnímu systému, na úrovni přístupu k aplikaci) jsou vázána na tyto role.

Zvláštní pozornost je zejména věnována při obsazování rolí s možností přístupu k centrálním systémům PostSignum QCA, tedy i všem systémům vyhrazeným pro provoz PostSignum Root QCA.

### 5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

V PostSignum QCA jsou definovány činnosti vyžadující přítomnost více než jedné osoby. Jedná se zejména o činnosti, při kterých se manipuluje se soukromým klíčem certifikační autority a s kryptografickým modulem použitým pro generování a úschovu soukromého klíče (nástrojem pro vytváření elektronického podpisu) certifikační autority.



### 5.2.3 Identifikace a autentizace pro každou roli

Představitel každé role se musí při přístupu k prostředkům PostSignum QCA identifikovat a autentizovat. Každý uživatel má přidělenou jednoznačnou identifikaci ve všech systémech, ke kterým má přístup. V systémech PostSignum QCA je používána identifikace jménem resp. certifikátem a autentizace heslem resp. soukromým klíčem.

### 5.2.4 Role vyžadující rozdělení povinností

V PostSignum QCA jsou stanovena pravidla, podle kterých jsou obsazovány jednotlivé role, a rovněž byla stanovena pravidla pro separaci rolí. Tato pravidla jsou uvedena v dokumentu Organizační zajištění úlohy Kvalifikovaná certifikační autorita České pošty, s.p

## 5.3 Personální bezpečnost

Do rolí spojených s obsluhou PostSignum Root QCA (role zajišťující provoz a správu, které mají přímý přístup k systémům PostSignum Root QCA) mohou být jmenováni pouze zaměstnanci ČP.

### 5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

Role, zajišťující provoz, správu, údržbu a rozvoj systémů PostSignum QCA jsou obsazovány na základě procedur (např. vyžadování referencí, zkušební období apod.), které zajišťují, aby tyto funkce byly obsazovány důvěryhodnými a kvalifikovanými pracovníky. Obdobné procedury platí pro uzavírání smluv s externími spolupracovníky nebo smluvními partnery.

V případě, že daná osoba není zaměstnancem České pošty, s. p., ale jejího smluvního partnera, uplatní se uvedené požadavky v příslušném rozsahu u daného partnera.

### 5.3.2 Posouzení spolehlivosti osob

Do rolí obsluhy PostSignum QCA jsou jmenovány výhradně osoby, které jsou delší dobu zaměstnány v České poště, s. p. a mají dobré pracovní a osobní reference.

V případě, že daná osoba není zaměstnancem České pošty, s. p., ale jejího smluvního partnera, uplatní se uvedené požadavky v příslušném rozsahu u daného partnera.

### 5.3.3 Požadavky na přípravu pro výkon role, vstupní školení

Všichni pracovníci, podílející se na provozu, správě, údržbě a rozvoji systémů PostSignum QCA, jsou vyškoleni. Součástí školení je i školení o bezpečnosti systému a o chování v havarijních situacích.

U rolí určených manažerem QCA může být školení nahrazeno prokazatelným seznámením pracovníka se všemi dokumenty upravujícími provoz QCA se vztahem k příslušné roli.

V případě, že daná osoba není zaměstnancem České pošty, s. p., ale jejího smluvního partnera, uplatní se uvedené požadavky v příslušném rozsahu u daného partnera.

### 5.3.4 Požadavky a periodicita školení

V PostSignum QCA existuje program vytváření, udržování a prohlubování bezpečnostního vědomí, diferencovaný podle rolí.

Manažer QCA v pravidelných intervalech (zejména při změnách v postupech PostSignum QCA, minimálně však jednou za dva roky) organizuje školení obsluhy.

### 5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Požadavky na rotaci pracovníků a její frekvenci nejsou definovány.

### 5.3.6 Postihy za neoprávněné činnosti zaměstnanců

Postihy za porušení pracovní kázně se řídí organizačními předpisy České pošty, s.p. nebo ustanoveními smlouvy mezi Českou poštou a smluvním partnerem.

### 5.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

Na smluvní (externí) pracovníky jsou uplatňována obdobná kritéria jako na zaměstnance České pošty, s.p.

### 5.3.8 Dokumentace poskytovaná zaměstnancům

Personál PostSignum QCA má k dispozici dokumentaci odpovídající jím obsazené roli, zejména

- bezpečnostní politiky,
- certifikační politiky,
- certifikační prováděcí směrnici,
- provozní dokumentaci – příručky a pracovní postupy pro obsluhu.

## 5.4 Auditní záznamy (logy)

Pro PostSignum QCA byl zpracován dokument Auditní a archivační politika (je přílohou dokumentu Systémová bezpečnostní politika), který popisuje zásady kontroly, auditu a archivace PostSignum QCA. Tento dokument je přístupný osobám, které provádějí kontrolu bezpečnostní shody PostSignum QCA. Tato kapitola vychází z dokumentu Auditní a archivační politika a poskytuje stručný přehled základních zásad uplatňovaných při kontrole PostSignum QCA.

### 5.4.1 Typy zaznamenávaných událostí

Pro potřeby kontroly a případné analýzy a vyšetření mimořádných událostí (obecně pro zajištění možnosti prokázat sled operací PostSignum QCA a jejich přiřazení osobě, která je vyvolala) jsou vedeny záznamy o událostech při vydání certifikátů, ukončení platnosti certifikátů, nakládání s klíči a certifikáty PostSignum QCA a dalších významných událostech (např. ukončení činnosti certifikační autority).

Auditní záznamy v písemné podobě musí být podepsány a musí uvádět jméno pracovníka, který záznam pořídil.

### 5.4.2 Periodicita zpracování záznamů

Auditní záznamy jsou kontrolovány osobami v odpovídající roli pověřené tímto úkolem v intervalech definovaných Systémovou bezpečnostní politikou. Dále podléhají interní a externí kontrole.

### 5.4.3 Doba uchování auditních záznamů

Auditní záznamy jsou uchovávány po dobu deseti let, pokud jiný předpis nestanoví dobu delší.

#### 5.4.4 Ochrana auditních záznamů

Auditní záznamy jsou uloženy tak, aby byly ochráněny proti krádeži, modifikaci a zničení úmyslnému i neúmyslnému (ohněm, vodou).

Auditní záznamy v podobě datových souborů jsou archivovány na nepřepisovatelných médiích.

#### 5.4.5 Postupy pro zálohování auditních záznamů

Auditní záznamy v písemné podobě nejsou obecně zálohovány; jsou pouze archivovány. Důležité auditní záznamy v písemné podobě spojené s vydáním certifikátů jsou uchovávány ve dvou kopiích, které jsou uloženy v různých lokalitách.

Auditní záznamy v elektronické podobě jsou zálohovány ve formě zálohování archivů vytvářených po každé změně v systémech PostSignum Root QCA.

#### 5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

Auditní záznamy jsou interně shromažďovány v rámci jednotlivých systémů PostSignum QCA.

#### 5.4.7 Postup při oznamování události subjektu, který ji způsobil

Subjektu, který způsobil událost zaznamenanou v auditním logu, není tato skutečnost nijak oznamována.

#### 5.4.8 Hodnocení zranitelnosti

Auditní záznamy jsou v pravidelných intervalech procházeny, kontrolovány a analyzovány na výskyt záznamů o nestandardních událostech, které mohou znamenat pokus o narušení bezpečnosti. Dále jsou definovány postupy, jak v těchto případech dále postupovat.

Zprávy o nestandardních událostech jsou mj. předávány i Auditorovi QCA.

### 5.5 Uchovávání informací a dokumentace

Pro PostSignum QCA byl zpracován dokument Auditní a archivační politika, který popisuje zásady kontroly, auditu a archivace v PostSignum QCA. Tento dokument je mj. přístupný osobám, které provádějí kontrolu PostSignum QCA.

#### 5.5.1 Typy informací a dokumentace, které se uchovávají

V PostSignum QCA se archivují tyto záznamy:

- programové vybavení a data, včetně vydaných certifikátů a CRL,
- veškerá dokumentace související s registrací žádosti o certifikát, včetně smluv,
- záznamy o obsazování rolí PostSignum QCA a záznamy o školení obsluhy,
- logy automaticky vytvářené komponentami informačního systému PostSignum QCA.

#### 5.5.2 Doba uchování uchovávaných informací a dokumentace

Programové vybavení, data a auditní záznamy se archivují po dobu deseti let.

### 5.5.3 Ochrana úložiště uchovávaných informací a dokumentace

Archiv je zabezpečen pomocí opatření technické a objektové bezpečnosti. Je rovněž chráněn proti vlivům prostředí, jako jsou teplota, vlhkost atd.

### 5.5.4 Postupy při zálohování uchovávaných informací a dokumentace

Zálohovací procedury archivu jsou upraveny samostatným dokumentem Auditní a archivační politika, který je mj. přístupný osobám provádějícím kontrolu PostSignum QCA.

### 5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

V PostSignum QCA nejsou časová razítka používána.

### 5.5.6 Systém shromažďování uchovávaných informací a dokumentace (interní nebo externí)

V prostředí PostSignum QCA jsou auditní záznamy shromažďovány a přesouvány do archivu QCA v souladu s postupy uvedenými v dokumentu Auditní a archivační politika.

### 5.5.7 Postupy pro získání a ověření uchovávaných informací a dokumentace

Archivy dat a programového vybavení jsou umístěny v k tomu určených trezorech.

V každé lokalitě, kde je umístěn trezor, musí být veden protokol o uložených archivních médiích, do kterého jsou zaznamenávány veškeré manipulace s uloženými médii.

Přístup k archivům je omezen na osoby v odpovídajících rolích. Ostatním osobám povoluje přístup do trezoru bezpečnostní administrátor QCA. O každém takto povoleném přístupu do trezoru je pořizován písemný záznam.

## 5.6 Výměna dat pro ověřování elektronických značek v nadřízeném kvalifikovaném systémovém certifikátu poskytovatele

Platnost klíčů certifikačních autorit v hierarchii PostSignum QCA je omezena.

S dostatečným předstihem, avšak nejméně 1 rok před vypršením platnosti certifikátu PostSignum Root QCA se musí uskutečnit ceremoniál vydání nového certifikátu. Výsledkem ceremoniálu bude vytvořený nový samopodepsaný certifikát kořenové certifikační autority, který bude zveřejněn způsobem popsáným v kapitole 2.

Plánovaná výměna klíčů certifikační autority musí být oznámena zákazníkům nejpozději 6 měsíců před vydáním nového certifikátu PostSignum Root QCA. Toto oznámení bude (včetně důvodu ukončení platnosti certifikátu) zveřejněno na webových stránkách PostSignum QCA a na všech pracovištích registrační autority PostSignum QCA.

Po ukončení potřeby používání původních dat pro vytváření elektronických značek Česká pošta prokazatelně tato data, která sloužila pro podepisování kvalifikovaných certifikátů a seznamů zneplatněných certifikátů, zničí a o tomto zničení provede záznam.

Tento postup bude také použit v případě, kdy bude nutné provést výměnu dat z důvodu nedostatečnosti záruk poskytovaných použitým algoritmem nebo jeho parametrů (např. velikostí modulu).

## 5.7 Obnova po havárii nebo kompromitaci

Pro PostSignum QCA byly vypracovány dokumenty popisující zvládnání krizových situací a postupy pro následnou obnovu.

Tato dokumentace je mj. přístupná pro osoby provádějící kontrolu PostSignum QCA.

Personál PostSignum QCA je řádně vyškolen, jak postupovat v případě havárie. Test havarijního plánu se provádí minimálně jedenkrát ročně.

### 5.7.1 Postup v případě incidentu a kompromitace

Zabezpečení prostředků certifikační autority po živelné katastrofě nebo jiné mimořádné události je rozpracováno v dokumentech Krizový plán ochrany objektu a Plán zvládnání krizových situací a plán obnovy.

### 5.7.2 Poškození výpočetních prostředků, softwaru nebo dat

Zabezpečení prostředků certifikační autority po živelné katastrofě nebo jiné mimořádné události je rozpracováno v dokumentech Krizový plán ochrany objektu a Plán zvládnání krizových situací a plán obnovy.

### 5.7.3 Postup při kompromitaci dat pro vytváření elektronických značek poskytovatele

V případě podezření na kompromitaci soukromého klíče PostSignum Root QCA budou písemně nebo elektronicky informováni všichni držitelé certifikátů, orgán určený [ZoEP] a subjekty, které mají uzavřenou smlouvu přímo se vztahující k poskytování certifikačních služeb o mimořádném ukončení činnosti této autority; oznámení bude rovněž zveřejněno na webových stránkách PostSignum QCA, na všech pracovištích registrační autority PostSignum QCA a v jednom celostátně vydávaném deníku. Součástí oznámení bude i důvod ukončení platnosti certifikátu certifikační autority.

Jako technické opatření provede poskytovatel certifikačních služeb zneplatnění certifikátu PostSignum Root QCA, platných certifikátů všech podřízených certifikačních autorit a všech jimi vydaných platných certifikátů; zneplatněné certifikáty budou neprodleně zveřejněny na příslušném CRL.

Po zveřejnění informace o mimořádném ukončení činnosti končí platnost všech certifikátů vydaných PostSignum Root QCA i podřízenými certifikačními autoritami.

Česká pošta prokazatelně zničí data pro vytváření elektronických značek PostSignum Root QCA, která sloužila pro podepisování kvalifikovaných certifikátů a seznamů zneplatněných certifikátů, u nichž existuje podezření na kompromitaci, a o tomto zničení provede záznam.

Tento postup bude také použit v případě, kdy dojde k náhlému oslabení algoritmu použitého pro vytváření elektronických značek, které nepopíratelně zpochybní důvěryhodnost vydávaných certifikátů a seznamů vydávaných certifikátů.

### 5.7.4 Schopnost obnovit činnost po havárii

Pokračování procesů certifikační autority po havárii závisí na typu havárie a jejích následcích a je věcí rozhodnutí managementu České pošty. O rozhodnutí managementu musí být s minimální prodlevou informováni všichni zákazníci PostSignum QCA.

Pokud management České pošty nerozhodne o ukončení provozu PostSignum QCA, nepřekročí doba výpadku služeb PostSignum QCA 20 pracovních dní.

## 5.8 Ukončení činnosti CA nebo RA

### 5.8.1 Ukončení činnosti kořenové certifikační autority

Ukončení činnosti PostSignum Root QCA musí být písemně oznámeno všem držitelům platných certifikátů, orgánu určeného [ZoEP] a subjektům, které mají uzavřenou smlouvu přímo se vztahující k poskytování certifikačních služeb a rovněž zveřejněno na webových stránkách PostSignum QCA a na všech pracovištích registrační autority PostSignum QCA. V případě, že součástí ukončení činnosti autority je i ukončení platnosti jejího certifikátu, musí být součástí oznámení i tato informace včetně příslušného důvodu ukončení platnosti. Dokud je platný alespoň jeden certifikát vydaný PostSignum Root QCA, musí PostSignum Root QCA zajišťovat alespoň funkci zneplatnění certifikátu a vydání CRL.

Pokud PostSignum Root QCA tuto funkci není schopna zajistit po celou dobu platnosti vydaných certifikátů, musí o této skutečnosti informovat držitele platných certifikátů spolu s uvedením data, do kdy bude funkce poskytována. Toto datum může být nejdříve 6 měsíců ode dne zaslání oznámení. K tomuto datu PostSignum Root QCA zneplatní všechny dosud platné vydané certifikáty a vydá poslední CRL. Teprve poté může být činnost PostSignum Root QCA ukončena.

V tomto případě budou smlouvy o poskytování certifikačních služeb ukončeny ze strany ČP dohodou nebo výpovědí.

Následně ČP prokazatelně zničí data pro vytváření elektronických značek PostSignum Root QCA, která sloužila pro označování kvalifikovaných certifikátů a seznamů zneplatněných certifikátů, a o tomto zničení provede záznam. Záznamy budou uchovávány v souladu s ustanoveními této certifikační politiky uvedenými v kapitole 5.4.

### 5.8.2 Ukončení činnosti poskytovatele certifikačních služeb

Činnost poskytovatele certifikačních služeb bude ukončena v souladu s §13 zákona o elektronickém podpisu [ZoEP].

### 5.8.3 Odnětí akreditace

V případě odnětí akreditace musí být informace o odnětí akreditace písemně nebo elektronicky oznámena všem držitelům platných certifikátů a subjektům, které mají uzavřenou smlouvu přímo se vztahující k poskytování certifikačních služeb a zveřejněna na webových stránkách PostSignum QCA, na všech pracovištích registrační autority PostSignum QCA a dalšími způsoby uvedenými ve § 10, odst. 3 [V378]. Součástí informace bude i sdělení, že kvalifikované certifikáty vydané tímto poskytovatelem nelze nadále používat podle §11 odst. 1 [ZoEP] a vydané kvalifikované systémové certifikáty nelze nadále používat podle § 11 odst. 2 [ZoEP].

O dalším postupu v tomto případě rozhodne management ČP na základě příslušného rozhodnutí orgánu určeného [ZoEP].

## 6 TECHNICKÁ BEZPEČNOST

### 6.1 Generování a instalace párových dat

Klíčové páry certifikačních autorit v hierarchii PostSignum QCA jsou generovány v odpovídajícím hardwarovém modulu; klíčové páry obsluhy jsou generovány v čipových kartách.

### 6.1.1 Generování párových dat

Klíčové páry certifikačních autorit v hierarchii PostSignum QCA jsou generovány a uloženy v hardwarovém kryptografickém modulu splňujícím požadavky [V378]. Generování těchto klíčových párů probíhá kontrolovaným procesem, na jehož průběh dohlíží Manažer QCA a Auditor QCA.

Klíčové páry jednotlivých komponent nebo systémů PostSignum QCA (infrastrukturní klíče) jsou generovány v kontrolovaném prostředí systémů PostSignum QCA. Tyto klíčové páry jsou uloženy v kryptografickém modulu; pro přístup k těmto klíčovým párům je nutné vložit čipovou kartu obsluhy a zadat PIN.

Klíčové páry operátorů PostSignum QCA (včetně operátorů RA; kontrolní klíče) jsou generovány ve vyhrazených čipových kartách, které svou konstrukcí neumožňují export soukromých klíčů. Pro použití soukromých klíčů je vždy nutné zadat PIN. Čipové karty jsou následně předány operátorům osobně nebo prostřednictvím sledovatelné zásilky odděleně od přístupového PINu.

### 6.1.2 Předání dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek podepisující nebo označující osobě

PostSignum QCA neposkytuje službu generování klíčových párů pro žadatele o certifikát.

### 6.1.3 Předání dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek poskytovateli certifikačních služeb

Veřejný klíč žadatele je poskytovateli certifikačních služeb doručen v elektronické podobě, v žádosti o certifikát ve formátu PKCS#10.

### 6.1.4 Poskytování dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek certifikační autoritou spoléhajícím se stranám

Certifikáty certifikačních autorit jsou zveřejněny způsobem popsáním v kapitole 2.

### 6.1.5 Délky párových dat

Klíče certifikačních autorit v hierarchii PostSignum mají pro algoritmus RSA délku modulu 2048 bitů.

### 6.1.6 Generování parametrů dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek a kontrola jejich kvality

Parametry používané při vytváření veřejných klíčů komponent PostSignum QCA jsou generovány odpovídajícím softwarovým a hardwarovým vybavením. Použité algoritmy a jejich parametry odpovídají požadavkům [V378].

Kvalita parametrů klíčů generovaných v rámci PostSignum QCA je automaticky testována použitým programovým vybavením.

### 6.1.7 Omezení pro použití dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek

Veřejné klíče podřízených certifikačních autorit mohou být použity pouze v souladu s pravidly popsanými v kapitole 1.4

## 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

Kryptografický modul použitý pro generování a úschovu soukromého klíče certifikačních autorit (nástroj pro vytváření elektronického podpisu) působících v hierarchii PostSignum splňuje požadavky standardu FIPS 140-2 Level 3 a byla mu orgánem podle [ZoEP] vyslovena shoda.

### 6.2.2 Sdílení tajemství

Soukromý klíč certifikační autority je během provozu uložen v aktivovaném a konfigurovaném kryptografickém modulu (nástroji pro vytváření elektronického podpisu), k jehož zapnutí a vypnutí postačuje jedna osoba.

K aktivování kryptografického modulu (nástroje pro vytváření elektronického podpisu) a k obnově soukromého klíče po havárii (případně v jiném kryptografickém modulu) je zapotřebí součinnosti několika, minimálně však tří osob.

### 6.2.3 Úschova dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Službu, která by vyžadovala uschování soukromých klíčů, PostSignum QCA neposkytuje.

### 6.2.4 Zálohování dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Soukromý klíč certifikační autority je zálohován v zašifrované formě; k šifrování je použit symetrický algoritmus AES. Zašifrované klíče jsou uloženy na pevném disku zařízení obsahujícího příslušný kryptografický modul. Zálohovat tyto klíče může jedna osoba; obnovit do aktivovaného modulu, ze kterého zálohy pocházejí, také.

Při obnově zálohovaných klíčů do nového nebo inicializovaného modulu je zapotřebí součinnosti minimálně tří osob.

### 6.2.5 Uchovávání dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Soukromé klíče certifikačních autorit v hierarchii PostSignum nejsou archivovány. Po ukončení provozu certifikační autority jsou protokolárně zničeny.

### 6.2.6 Transfer dat pro vytváření elektronických značek do kryptografického modulu nebo z kryptografického modulu

Soukromý klíč certifikační autority je generován v kryptografickém modulu (bezpečném kryptografickém modulu) a veškeré operace s nezašifrovaným klíčem se provádějí pouze v tomto modulu. Klíč opouští kryptografický modul pouze v zašifrované podobě na zálohách vytvářených a chráněných v souladu s ustanoveními dokumentů Systémová bezpečnostní politika, Provozní a bezpečnostní procedury a Auditní a archivační politika (součást [SBP]).

Klíč je do původního kryptografického modulu vkládán se záloh po autentizaci jednoho pracovníka s přístupem k zálohám klíčů a ke kryptografickému modulu.

Klíč je do nového nebo inicializovaného kryptografického modulu vkládán se záloh po autentizaci dvou pracovníků, kteří nemají přístup k záloze soukromého klíče a kteří nemají právo na aktivaci soukromého klíče (spuštění procesu certifikační autority).



### 6.2.7 Uložení dat pro vytváření elektronických značek v kryptografickém modulu

Soukromý klíč certifikační autority je během provozu uložen v nezašifrovaném tvaru v aktivovaném a konfigurovaném kryptografickém modulu (bezpečném kryptografickém modulu), k jehož zapnutí a vypnutí postačuje jedna osoba.

K aktivování kryptografického modulu (bezpečného kryptografického modulu) a k obnově soukromého klíče po havárii (případně v jiném kryptografickém modulu) je zapotřebí součinnosti několika, minimálně však tří osob.

### 6.2.8 Postup při aktivaci dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Soukromý klíč certifikační autority je aktivován autorizovanou obsluhou v souladu se Systémovou bezpečnostní politikou a Provozními a bezpečnostními procedurami. Tato aktivace pro PostSignum Root QCA je prováděna (kromě případů popsaných v Plánu zvládnání krizových situací a plánu obnovy) výhradně v rámci plánovaného spuštění za přítomnosti Manažera QCA a Auditora QCA, kteří dohlíží na kryptografický modul obsahující aktivovaný soukromý klíč až do okamžiku deaktivace.

### 6.2.9 Postup při deaktivaci dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Soukromý klíč certifikační autority je deaktivován autorizovanou obsluhou v souladu se Systémovou bezpečnostní politikou a Provozními a bezpečnostními procedurami.

### 6.2.10 Postup při zničení dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Soukromý klíč certifikační autority uložený v HSM modulu je zničen prostředky poskytovanými HSM modulem v případě ukončení činnosti certifikační autority, jejíž klíče jsou v HSM modulu uloženy. Toto zničení soukromého klíče se provádí autorizovanou obsluhou v souladu s ustanoveními dokumentu Systémová bezpečnostní politika a dokumentu Provozní a bezpečnostní procedury nebo na základě požadavku Manažera QCA.

Zničení soukromého klíče je provedeno uvedením HSM do inicializovaného stavu, kdy je pomocí mechanismů HSM bezpečně vymazán veškerý kryptografický materiál (včetně soukromého klíče CA). Zničení soukromého klíče zahrnuje i smazání zálohovaných kopií klíčů a deaktivaci karet použitých pro přístup ke klíčům.

### 6.2.11 Hodnocení kryptografických modulů

Vzhledem ke skutečnosti, že kryptografický modul užívaný k úschově soukromého klíče certifikační autority úspěšně prošel hodnocením podle standardu FIPS 140–2 na úroveň 3, nepředpokládá se, že by obsahoval závažné chyby na úrovni designu zařízení. Přesto se průběžně sleduje, zda nebyl objeven útok na toto zařízení, aby bylo možné včas na takové ohrožení reagovat.

## 6.3 Další aspekty správy párových dat

### 6.3.1 Uchovávání dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek

Veřejné klíče ve formě certifikátů vydaných autoritou PostSignum Root QCA jsou archivovány v souladu s Auditní a archivační politikou.

### 6.3.2 Maximální doba platnosti certifikátu vydaného podepisující nebo označující osobě a párových dat

Doba platnosti certifikátu vydaného podřízené certifikační autoritě je 10 let. Páry klíčů svázané s certifikáty mají stejnou dobu platnosti jako certifikáty.

### 6.4 Aktivační data

V systému PostSignum QCA jsou používána aktivační data různého charakteru, například přístupová hesla, PIN a jiné. Všechny aspekty týkající se aktivačních dat, jejich generování, instalace a používání, jsou popsány v Systémové bezpečnostní politice, Provozních a bezpečnostních procedurách a provozní dokumentaci.

#### 6.4.1 Generování a instalace aktivačních dat

Aktivační data jdou většinou vytvářena nebo zadávána pracovníkem, který je bude dále používat. V opačném případě, kdy je generuje jiný subjekt, jsou použita náhodná data splňující obecné požadavky na tato data a je definována povinnost tato náhodně generovaná data neprodleně změnit.

Všechna vytvářená aktivační data musí splňovat požadavky kladené na jejich délku nebo složení.

#### 6.4.2 Ochrana aktivačních dat

Všechna aktivační data musí být chráněna před prozračením neoprávněné osobě. Příslušné povinnosti v tomto smyslu mají všichni pracovníci PostSignum QCA a jsou uvedeny v Systémové bezpečnostní politice.

#### 6.4.3 Ostatní aspekty aktivačních dat

Ostatní aspekty týkající se aktivačních dat, jejich generování, instalace a používání, jsou popsány v Systémové bezpečnostní politice, Provozních a bezpečnostních procedurách a provozní dokumentaci.

### 6.5 Počítačová bezpečnost

#### 6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Pro každou komponentu v hierarchii PostSignum QCA jsou definována nastavení zajišťující bezpečnost dané komponenty na technologické úrovni, který vycházejí z požadavků [V378] a návazných dokumentů, a to zejména ze standardů

- CWA 14167-1 – Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements.
- ČSN ETSI TS 101 456 – Elektronické podpisy a infrastruktury; Požadavky na postupy certifikační autority vydávající kvalifikované certifikáty.

#### 6.5.2 Hodnocení počítačové bezpečnosti

Systém PostSignum QCA prošel po vybudování externí kontrolou bezpečnostní shody zaměřenou na splnění požadavků kladených legislativou na akreditovaného poskytovatele certifikačních služeb, a to zejména požadavků uvedených v

- [ZoEP],
- [V378],

- standardu CWA 14167-1 – Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements.
- standardu ČSN ETSI TS 101 456 – Elektronické podpisy a infrastruktury; Požadavky na postupy certifikační autority vydávající kvalifikované certifikáty.

Jádro certifikační autority, software UniCERT ve verzi 5.2.1, prošlo certifikací podle standardu Common Criteria s úrovní záruk EAL 4+.

## 6.6 Bezpečnost životního cyklu

### 6.6.1 Řízení vývoje systému

Implementace systému probíhala podle metodologie KeyStep, která byla vytvořena speciálně pro návrh a implementaci rozsáhlých PKI projektů. Vývoj dílčích aplikací probíhal v souladu s interní metodikou vývoje České pošty.

Následné změny jsou realizovány v souladu s definovaným změnovým řízením.

### 6.6.2 Kontroly řízení bezpečnosti

Bezpečnost systémů PostSignum QCA je ověřována provozními kontrolami zavedenými v rámci zavedeného systému řízení informační bezpečnosti podle ISO/IEC 27001:2005, kontrolami bezpečnostní shody prováděnými pracovníky kontroly ČP a externími audity, které provádí externí subjekt.

### 6.6.3 Řízení bezpečnosti životního cyklu

Součástí změnového řízení je i hodnocení dopadu změn na bezpečnost řešení. V případě velkých změn nebo po sérii menších změn je provedena rozdílová nebo opakovaná analýza rizik.

## 6.7 Síťová bezpečnost

Centrální systémy certifikační autority PostSignum Root QCA, které zajišťují vydávání certifikátů, nejsou připojeny k žádné síti.

## 6.8 Časová razítka

V PostSignum QCA nejsou časová razítka používána.

## 7 PROFILY CERTIFIKÁTU, SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ A OCSP

### 7.1 Profil certifikátu

PostSignum Root QCA vydává certifikáty odpovídající standardu X.509. Profil certifikátu podřízené certifikační autority je uveden v následující tabulce.

Tab. 2 Profil certifikátu podřízené certifikační autority

Název položky	Hodnota/příznak použití
Version	3 (0x2)
Serial Number	<i>PostSignum Root QCA přiřazuje každému vydanému certifikátu jednoznačné číslo.</i>
SignatureAlgorithm	Sha256WithRSAEncryption

Issuer	
Country	CZ
Organisation	Česká pošta, s.p. [IČ 47114983]
CN	PostSignum Root QCA 2
Validity	
Not Before	<i>Datum vydání - UTCTime</i>
Not After	<i>10 let od data vydání - UTCTime</i>
Subject	
Country	CZ
Organisation	Česká pošta, s.p. [IČ 47114983]
Locality	<i>Sídlo podřízené certifikační autority. Nepovinná položka</i>
OU	<i>Organizační jednotka, která provozuje CA. Nepovinná položka</i>
CN	<i>Jméno certifikační autority</i>
Subject Public Key Info	
Algorithm	rsaEncryption
SubjectPublicKey	<i>Veřejný klíč označující osoby</i>
Extensions	<i>rozšíření certifikátu podle tabulky 3</i>
Signature	<i>elektronická značka poskytovatele certifikačních služeb</i>

### 7.1.1 Číslo verze

PostSignum Root QCA vydává certifikáty vyhovující standardu X.509 verze 3.

### 7.1.2 Rozšiřující položky v certifikátu

Rozšiřující položky použité v certifikátu podřízené certifikační autority jsou uvedeny v následující tabulce.

Tab. 3 Rozšíření v certifikátu

Název rozšiřující položky	Hodnota/příznak použití	Kritická ano/ne
Authority Key Identifier		ne
Key Identifier	<i>používá se</i>	
AuthorityCertIssuer	<i>používá se</i>	
AuthorityCertSerialNumber	<i>používá se</i>	
Subject Key Identifier	<i>používá se</i>	ne
Key Usage		ano
DigitalSignature	Ne	
NonRepudiation	Ne	
KeyEncipherment	Ne	
DataEncipherment	Ne	
KeyAgreement	Ne	
KeyCertSign	Ano	
CRLSign	Ano	
CertificatePolicies		ne
Policy Identifier	2.5.29.32.0 (Any Policy)	
User Notice	Tento kvalifikovaný systémový certifikát byl vydán podle zákona 227/2000Sb. a navazných předpisů/This qualified system	

	certificate was issued according to Law No 227/2000Coll. and related regulations	
CRL Distribution Points		ne
URI	http://www.postsignum.cz/crl/psrootqca2.crl	
URI	http://www2.postsignum.cz/crl/psrootqca2.crl	
URI	http://postsignum.ttc.cz/crl/psrootqca2.crl	
Basic Constraints		ano
cA	TRUE	
PathLenConstraint	0	
AuthorityInfoAccess		
accessMethod	id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	
URI	http://www.postsignum.cz/crt/psrootqca2.crt	
accessMethod	id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	
URI	http://www2.postsignum.cz/crt/psrootqca2.crt	
accessMethod	id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	
URI	http://postsignum.ttc.cz/crt/psrootqca2.crt	

Poznámka: Některé položky certifikátu neobsahují diakritiku z důvodu lepší čitelnosti údajů v certifikátu v různých systémech.

### 7.1.3 Objektové identifikátory (dále „OID“) algoritmů

Algoritmům používaným v PostSignum QCA nejsou přiřazeny OID. V hierarchii PostSignum QCA se nepoužívají specifické algoritmy, které by vyvíjel provozovatel PostSignum QCA nebo jeho dodavatel, ale pouze algoritmy odpovídající požadavkům [V378].

### 7.1.4 Způsoby zápisu jmen a názvů

Pravidla pro zápis jmen a názvů jsou uvedena v odstavcích 3.1.1 až 3.1.4.

### 7.1.5 Omezení jmen a názvů

Jména a názvy uvedené v certifikátu musí přesně odpovídat údajům v dokladech předložených při registraci a podléhají schválení Komise pro certifikační politiky. Subjekt certifikátu musí obsahovat obchodní firmu nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen.

### 7.1.6 OID certifikační politiky

Ve vydávaných certifikátech pro podřízené certifikační autority je podle [RFC5280] uvedeno speciální označení politiky anyPolicy s OID 2.5.29.32.0

OID této politiky (dokumentu) je uvedeno v odstavci 1.2 (Tab. 1)

### 7.1.7 Rozšiřující položka „Policy Constraints“

Rozšiřující položka „Policy Constraints“ se v PostSignum QCA nepoužívá.

### 7.1.8 Syntaxe a sémantika rozšiřující položky kvalifikátorů politiky „Policy Qualifiers“

Rozšiřující položka „Policy Qualifier“ obsahuje ve formě User Notice informaci, že certifikát byl vydán jako kvalifikovaný systémový certifikát podle [ZoEP].

### 7.1.9 Způsob zápisu kritické rozšiřující položky „Certificate Policies“

Způsob zápisu rozšiřující položky „Certificate Policies“ je uveden v tabulce 3. Tato položka není označena jako kritická.

### 7.2 Profil seznamu zneplatněných certifikátů

Tab. 4 Profil CRL

Název položky	Hodnota/příznak použití
Version	2 (0x1)
Issuer Distinguished Name	
Country	CZ
Organisation	Česká pošta, s.p. [IČ 47114983]
CN	PostSignum Root QCA 2
Validity	
This Update	<i>Datum vydání</i>
Next Update	<i>Datum vydání + 12 měsíců</i>
RevokedCertificates	<i>opakující se položka pro každý zneplatněný certifikát</i>
UserCertificate	<i>sériové číslo zneplatněného certifikátu</i>
RevocationDate	<i>datum a čas zneplatnění</i>
CrlEntryExtensions	<i>rozšíření položky CRL podle tabulky 5</i>
CrlExtensions	<i>rozšíření CRL podle tabulky 5</i>
SignatureAlgorithm	Sha256WithRSAEncryption
Signature	<i>elektronická značka poskytovatele certifikačních služeb</i>

#### 7.2.1 Číslo verze

PostSignum Root QCA vydává seznamy zneplatněných certifikátů podle standardu X.509 verze 2.

#### 7.2.2 Rozšiřující položky seznamu zneplatněných certifikátů a záznamů v seznamu zneplatněných certifikátů

Tab. 5 Rozšíření v CRL

Název rozšiřující položky	Hodnota/příznak použití	Kritická ano/ne
Rozšíření položky (CrlEntryExtensions)		
InvalidityDate	<i>datum a čas vzniku události vedoucí ke zneplatnění certifikátu; volitelné rozšíření</i>	ne
ReasonCode	<i>důvod zneplatnění certifikátu</i>	ne
Rozšíření pro CRL (CrlExtensions)		
Authority Key Identifier		ne
Key Identifier	<i>používá se</i>	
AuthorityCertIssuer	<i>používá se</i>	
AuthorityCertSerialNumber	<i>používá se</i>	
CRL Number	<i>PostSignum Root QCA přiřadí každému CRL jednoznačné číslo</i>	ne

### 7.3 Profil OCSP

PostSignum QCA tuto službu neposkytuje.

#### 7.3.1 Číslo verze

PostSignum QCA tuto službu neposkytuje.

#### 7.3.2 Rozšiřující položky OCSP

PostSignum QCA tuto službu neposkytuje.

## 8 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

### 8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

V prostředí PostSignum QCA jsou pravidelně prováděny interní kontroly (jednou za 12 měsíců). Kromě těchto interních kontrol je jednou za 4 roky provedena externí kontrola. Tyto pravidelné kontroly mohou být podle potřeby doplněny další kontrolou, mimo jiné na základě rozhodnutí manažera QCA, managementu České pošty nebo odboru interního auditu České pošty, resp. odboru kontroly České pošty.

Součástí interní a externí kontroly je i kontrola bezpečnostní shody ve smyslu §8, odst. 2 [V378].

### 8.2 Identita a kvalifikace hodnotitele

Interní kontrolu provádějí pracovníci znalí problematiky PKI a proškolení pro daný úkol. Pracovníci provádějící kontrolu jsou, v důsledku organizačních změn v České poště, v dokumentaci QCA označováni jako Auditóři QCA.

Externím auditorem smí být pouze osoba nebo společnost znalá problematiky implementace PKI s dostatečnou zkušeností v této oblasti.

### 8.3 Vztah hodnotitele k hodnocenému subjektu

Interní kontrolu provádí zaměstnanci České pošty, s. p.

Externí kontrolu smí provádět pouze osoba nebo společnost nezávislá na České poště, s. p.

### 8.4 Hodnocené oblasti

Oblasti hodnocené v rámci pravidelných kontrol jsou specifikovány v Certifikační prováděcí směrnici a v příloze Systémové bezpečnostní politiky (Auditní a archivační politice).

### 8.5 Postup v případě zjištění nedostatků

Výsledky kontrol jsou předávány manažerovi QCA a bezpečnostnímu administrátorovi QCA, který zajistí nápravu zjištěných nedostatků.

V případě zjištění nedostatků, které závažně ovlivní schopnost PostSignum QCA dostát svým závazkům a požadavkům uvedeným v [ZoEP], přeruší PostSignum QCA vydávání certifikátů do doby, než budou nedostatky odstraněny.

## 8.6 Sdělování výsledků hodnocení

O provedení každé kontroly je vypracována podepsaná písemná zpráva, která je předána manažerovi QCA. Ten zajistí její distribuci a projednání. Pokud je součástí zprávy zpráva o kontrole bezpečnostní shody ve smyslu §8, odst. 2 [V378], zajistí manažer QCA její předání orgánu podle [ZoEP] do 30 dní od ukončení této kontroly bezpečnostní shody.

V případě, kdy je součástí zprávy samostatný výrok auditora, může manažer QCA rozhodnout o jeho zveřejnění.

## 9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

### 9.1 Poplatky

#### 9.1.1 Poplatky za vydání nebo obnovení certifikátu

Provozovatelem všech certifikačních autorit v hierarchii PostSignum QCA je Česká pošta, poplatky za vydávání certifikátů podřízených certifikačních autorit se neúčtují.

#### 9.1.2 Poplatky za přístup k certifikátu na seznamu vydaných certifikátů

Služba přístupu k certifikátu na seznamu vydaných certifikátů je poskytována bezplatně.

#### 9.1.3 Poplatky za informace o statutu certifikátu nebo o zneplatnění certifikátu

Služba zneplatnění certifikátu a informace o stavu certifikátu jsou poskytovány bezplatně.

#### 9.1.4 Poplatky za další služby

Provozovatelem všech certifikačních autorit v hierarchii PostSignum QCA je Česká pošta, poplatky za další služby se neúčtují.

#### 9.1.5 Jiná ustanovení týkající se poplatků (vč. refundací)

Viz ustanovení odstavce 9.1.1.

### 9.2 Finanční odpovědnost

#### 9.2.1 Krytí pojištěním

Česká pošta má sjednané pojištění odpovědnosti za škodu. Smlouva je uzavřena s následujícími pojišťovnami: Kooperativa, pojišťovna, a.s., Česká pojišťovna, a.s. a Česká podnikatelská pojišťovna, a.s.

Pro všechny zaměstnance České pošty je sjednáno pojištění odpovědnosti za škodu způsobenou zaměstnavateli při výkonu povolání. Smlouva je uzavřena s Českou podnikatelskou pojišťovnou, a.s.

#### 9.2.2 Další aktiva a záruky

Aktiva České pošty jsou uvedena ve Výroční zprávě. Výroční zpráva je uložena v obchodním rejstříku u Městského soudu v Praze pod spisovou značkou A7565.

Výroční zpráva je k nahlédnutí též na webových stránkách České pošty ([www.cpost.cz](http://www.cpost.cz)).



### 9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

PostSignum QCA tuto službu neposkytuje.

## 9.3 Citlivost obchodních informací

Provozovatelem všech certifikačních autorit v hierarchii PostSignum QCA je Česká pošta. V oblasti ochrany obchodních informací se uplatní ustanovení obecných interních předpisů ČP týkajících se klasifikace informací a jejich ochrany.

### 9.3.1 Výčet citlivých informací

Za důvěrné jsou považovány všechny informace s výjimkou informací uvedených v dokumentech s označením „Informace určené pro veřejnost“.

### 9.3.2 Informace mimo rámec citlivých informací

Za důvěrné se nepovažují informace, které jsou klasifikované a označené jako „Informace určené pro veřejnost“.

### 9.3.3 Odpovědnost za ochranu citlivých informací

Odpovědnost za zpracování důvěrných informací v PostSignum QCA nese Česká pošta, jakožto poskytovatel certifikačních služeb, všichni její zaměstnanci a smluvní partneři.

## 9.4 Ochrana osobních údajů

Česká pošta zajišťuje ochranu osobních údajů osob, k nimž získá přístup při poskytování certifikačních služeb. Zásady ochrany osobních údajů jsou obsaženy v této certifikační politice, v Certifikační prováděcí směrnici [CPS] a vycházejí z příslušných ustanovení zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.

Obecně platí, že při provozu PostSignum Root QCA, vydávání a následné správě certifikátů vydaných touto autoritou jsou ukládány výhradně osobní údaje pracovníků ČP.

### 9.4.1 Politika ochrany osobních údajů

Česká pošta zajišťuje ochranu osobních údajů osob, k nimž získá přístup při poskytování certifikačních služeb. Zásady ochrany osobních údajů vycházejí z příslušných ustanovení [Z101].

### 9.4.2 Osobní údaje

Za osobní údaje jsou považovány informace, které spadají pod ochranu [Z101]. Zejména se jedná o veškeré informace týkající se určené nebo určitelné fyzické osoby (zaměstnance ČP).

### 9.4.3 Údaje, které nejsou považovány za citlivé

Za citlivé nejsou považovány informace, které nespádají pod ochranu [Z101].

### 9.4.4 Odpovědnost za ochranu osobních údajů

Odpovědnost za ochranu osobních údajů zpracovávaných v systémech PostSignum QCA nese Česká pošta, jakožto poskytovatel certifikačních služeb, všichni její zaměstnanci a smluvní partneři v rozsahu [Z101].

#### 9.4.5 Oznámení o používání důvěrných informací a souhlas s používáním citlivých informací

Žadatel o certifikát dává během procesu registrace žádosti o certifikát České poště souhlas se zpracováním osobních údajů nutných pro jednoznačnou identifikaci v rámci České pošty, s.p. (jméno, příjmení a osobní číslo).

#### 9.4.6 Poskytnutí citlivých informací pro soudní či správní účely

Veškeré informace zpracovávané v PostSignum QCA jsou zpřístupněny orgánům zmocněným ze zákona v případech, kdy to zákon vyžaduje, a do té míry, do jaké to zákon vyžaduje. Zpřístupnění informací zajistí manažer QCA poté, co orgány zmocněné ze zákona prokáží své zmocnění způsobem obvyklým v těchto případech.

#### 9.4.7 Jiné okolnosti zpřístupňování osobních údajů

V této oblasti je postupováno podle příslušných ustanovení [Z101] a interních předpisů České pošty, s. p. upravujících problematiku ochrany osobních údajů.

#### 9.5 Práva duševního vlastnictví

Tato certifikační politika a veškeré související dokumenty jsou chráněny autorskými právy České pošty a představují významné know-how České pošty. Česká pošta je rovněž nositelem výlučných práv k informačnímu systému pro provoz PostSignum QCA a ke struktuře, organizaci, vzhledům obrazovek a obsahu webových stránek PostSignum QCA.

#### 9.6 Zastupování a záruky

Česká pošta zaručuje, že splní veškeré povinnosti uložené touto certifikační politikou a mandatorními ustanoveními příslušných právních předpisů.

Česká pošta poskytuje výše uvedené záruky po celou dobu platnosti smlouvy o poskytování certifikačních služeb.

##### 9.6.1 Zastupování a záruky CA

Viz ustanovení odst. 9.6.

##### 9.6.2 Zastupování a záruky RA

Viz ustanovení odst. 9.6.

##### 9.6.3 Zastupování a záruky držitele certifikátu, podepisující nebo označující osoby

Viz ustanovení odst. 9.6.

##### 9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strana ručí za naplnění všech povinností, které jsou na spoléhající se stranu kladeny před použitím kvalifikovaného certifikátu. Tyto povinnosti jsou uvedeny v této certifikační politice, především v odst. 4.5.2.

##### 9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Viz ustanovení odst. 9.6.

## 9.7 Zřeknutí se záruk

Záruky uvedené v čl. 9.6 výše jsou výlučnými zárukami České pošty a Česká pošta jiné záruky neposkytuje.

Česká pošta neodpovídá za vady poskytnutých služeb vzniklé z důvodu nesprávného nebo neoprávněného využívání služeb, zejména za provozování v rozporu s podmínkami uvedenými v této certifikační politice, jakož i za vady vzniklé z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení aj.

## 9.8 Omezení odpovědnosti

Česká pošta neodpovídá za škodu vyplývající z použití kvalifikovaného certifikátu, pokud došlo ze strany spoléhající se osoby k nedodržení omezení pro jeho použití, uvedených v této certifikační politice a zveřejněných na webových stránkách PostSignum QCA.

Česká pošta bude průběžně s rostoucími provozními zkušenostmi s poskytováním certifikačních služeb ověřovat, zda podmínky omezení odpovědnosti České pošty uvedené v tomto ustanovení odpovídají obvyklým podmínkám na trhu a přiměřenému obchodnímu riziku České pošty.

Ustanovení tohoto článku zůstávají v platnosti i po ukončení platnosti této certifikační politiky.

## 9.9 Odpovědnost za škodu, náhrada škody

Pokud nevyplývá z mandatorních ustanovení platných právních předpisů jinak, odpovídá Česká pošta spoléhající se osobě za škodu způsobenou porušením povinností České pošty v souvislosti s poskytováním certifikačních služeb.

## 9.10 Doba platnosti, ukončení platnosti

### 9.10.1 Doba platnosti

Doba platnosti této certifikační politiky je od data vydání uvedeného v odst. 1.2 do odvolání.

### 9.10.2 Ukončení platnosti

Platnost dokumentu je ukončena v případě

- jeho nahrazení novější verzí nebo
- ukončení poskytování služeb Českou poštou, s. p. jako poskytovatelem certifikačních služeb.

### 9.10.3 Důsledky ukončení a přetrvání závazků

V případě ukončení platnosti tohoto dokumentu v důsledku ukončení poskytování služeb zůstávají v platnosti omezení a ustanovení uvedená v kapitole 9, která se týkají obchodních a právních záležitostí.

## 9.11 Komunikace mezi zúčastněnými subjekty

### 9.11.1 Komunikace s poskytovatelem certifikačních služeb

Veškeré informace, které chce poskytovatel certifikačních služeb sdělit spoléhajícím se osobám, zveřejní na svých webových stránkách a na vývěskách na pracovištích registračních autorit. Závažné informace, jako například podezření na kompromitaci klíče některé z certifikačních autorit hierarchie PostSignum, sděluje poskytovatel certifikačních služeb opět na webových stránkách a způsoby popsány v odstavci 2.2.

### 9.11.2 Komunikace v rámci systému PostSignum QCA

Komunikace v systému PostSignum QCA se řídí platnými předpisy České pošty a interními dokumenty úlohy PostSignum QCA.

### 9.11.3 Komunikační jazyk

Veškerá komunikace v systému PostSignum QCA musí probíhat v českém jazyce, pokud se obě strany nedohodnou jinak.

## 9.12 Změny

### 9.12.1 Postup při změnách

Postupy pro zapracování změn jsou uvedeny v odst. 1.5.

### 9.12.2 Postup při oznamování změn

Vydání nové certifikační politiky se změněným OID (viz následující odstavec) bude oznámeno v aktualitách na webových stránkách PostSignum QCA.

V případě identifikace oslabení záruk poskytovaných používanými kryptografickými algoritmy vyžadující neodkladný zásah budou písemně nebo elektronicky informováni všichni držitelé certifikátů, orgán určený [ZoEP] a subjekty, které mají uzavřenou smlouvu přímo se vztahující k poskytování certifikačních služeb. Oznámení bude rovněž zveřejněno na webových stránkách PostSignum QCA, na všech pracovištích registrační autority PostSignum QCA. Na toto oznámení mohou navazovat další akce, které jsou popsány v této certifikační politice.

### 9.12.3 Okolnosti, při kterých musí být změněn OID

Česká pošta, s.p. přiřadila dle svých interních pravidel identifikátory objektů (OID) užívané v prostředí PostSignum QCA.

OID jsou přiřazeny:

- PostSignum Root QCA,
- každé certifikační autoritě, které PostSignum Root QCA vydala certifikát, zejména certifikační autoritě PostSignum Qualified CA,
- každé certifikační politice, podle které jsou vydávány certifikáty v rámci PostSignum QCA.

OID nejsou přiřazeny registračním autoritám ani certifikační prováděcí směrnicí.

Jakákoliv změna v certifikační politice vyvolá změnu verze dokumentu; větší změna v certifikační politice, která má dopad na použitelnost certifikátu, záruky, odpovědnost nebo procesy, vyvolá i změnu OID.

## 9.13 Řešení sporů

V případě vzniku sporu mezi provozovatelem PostSignum Root QCA a podřízenou certifikační autoritou (žadatelem) je možné se obrátit na nadřízené pracovníky manažera PostSignum Root QCA.

## 9.14 Rozhodné právo

Činnost PostSignum QCA se řídí právním řádem České republiky.

## 9.15 Shoda s právními předpisy

Činnost PostSignum QCA je v souladu s právním řádem České republiky, zejména se zákonem č.227/2000 Sb. o elektronickém podpisu ve znění pozdějších předpisů a vyhláškou Ministerstva informatiky č. 378/2006 Sb. ze dne 19. července 2006 o postupech kvalifikovaných poskytovatelů certifikačních služeb.

Struktura této certifikační politiky je v souladu se strukturou uvedenou v příloze 2 [V378].

## 9.16 Další ustanovení

### 9.16.1 Rámcová dohoda

Žádná ustanovení v tomto odstavci.

### 9.16.2 Postoupení práv

Česká pošta může přenést část nebo všechny povinnosti poskytovatele certifikačních služeb na jiný právní subjekt, u kterého je zajištěna stejná úroveň bezpečnosti i poskytovaných služeb. Vztahy mezi Českou poštou a tímto subjektem budou upraveny zvláštní smlouvou.

V případě ukončení činnosti kvalifikovaného poskytovatele certifikačních služeb vyvine Česká pošta přiměřené úsilí pro převzetí správy platných kvalifikovaných certifikátů a související agendy jiným kvalifikovaným poskytovatelem certifikačních služeb. V tomto případě budou vztahy mezi tímto kvalifikovaným poskytovatelem certifikačních služeb a Českou poštou rovněž upraveny zvláštní smlouvou.

Převzetí části nebo všech povinností poskytovatele certifikačních služeb třetí stranou neomezuje služby ani záruky poskytované Českou poštou vzhledem k zákazníkům a spoléhajícím se stranám.

### 9.16.3 Oddělitelnost ustanovení

Smlouva o poskytování certifikačních služeb uzavřená mezi zákazníkem a Českou poštou zůstává platná i v případě, že jakákoliv její dílčí část pozbude platnost, pokud se obě strany nedohodnou jinak.

### 9.16.4 Zřeknutí se práv

Žádná ustanovení v tomto odstavci.

### 9.16.5 Vyšší moc

Česká pošta nenese odpovědnost za porušení svých povinností způsobené zásahy vyšší moci, jako jsou například přírodní katastrofy velkého rozsahu, stávky, občanské nepokoje nebo válečný stav.

## 9.17 Další opatření

### 9.17.1 Řídící dokumenty

Při tvorbě certifikačních politik a certifikační prováděcí směrnice bylo zejména přihlíženo k následujícím dokumentům:

- zákon č. 227/2000 Sb. o elektronickém podpisu v platném znění;
- vyhláška Ministerstva informatiky č. 378/2006 Sb. ze dne 19. července 2006 o postupech kvalifikovaných poskytovatelů certifikačních služeb;

- CWA 14167-1: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements
- ČSN ETSI TS 101 456 – Elektronické podpisy a infrastruktury; Požadavky na postupy certifikační autority vydávající kvalifikované certifikáty;
- ČSN ISO/IEC TR 13335: Informační technologie – Směrnice pro řízení bezpečnosti IT
- ČSN ISO/IEC 17799: Informační technologie – Bezpečnostní techniky – Soubor postupů pro management bezpečnosti informací
- RFC 2511 – Internet X.509 Certificate Request Message Format
- RFC 3280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- RFC 3739 – Internet X.509 Public Key Infrastructure: Qualified Certificates Profile

#### 9.17.2 Odkazy a literatura

- [ZoEP] Zákon č. 227/2000 Sb. o elektronickém podpisu v platném znění
- [V378] Vyhláška Ministerstva informatiky č. 378/2006 Sb. ze dne 19. července 2006 o postupech kvalifikovaných poskytovatelů certifikačních služeb
- [VOP] Všeobecné obchodní podmínky elektronických služeb České pošty, s. p.
- [Z101] Zákon č. 101/2000 Sb. o ochraně osobních údajů v aktuálním znění
- [RFC3280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- [RFC5280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile