# Certifikační politika PostSignum Qualified CA pro certifikáty TSA

Verze 1.4

**OBSAH**

# Evidence revizí a změn

| Verze | Účinnost od | Důvod a popis změny | Autor | Schválil |
|---|---|---|---|---|
| 1.0 | 22.5.2009 | První verze | PCA ČP | PAA ČP |
| 1.1 | 22.6.2009 | Aktualizace dokumentu | PCA ČP | PAA ČP |
| 1.2 | 8.1.2010 | Aktualizace dokumentu | PCA ČP | PAA ČP |
| 1.3 | 1.7.2012 | Aktualizace dokumentu | PCA ČP | PAA ČP |
| 1.4 | 1.4.2014 | Aktualizace dokumentu | PCA ČP | PAA ČP |

# 1 ÚVOD

Tento dokument stanoví pravidla a postupy pro vydávání kvalifikovaných systémových certifikátů pro ověření elektronické značky kvalifikovaného časového razítka.

Jméno poskytovatele služby vydávání časových razítek je uvedeno v jedné z položek subjektu certifikátu.

## 1.1 Přehled

Česká pošta, s.p. (dále i Česká pošta či ČP) provozuje certifikační autoritu s názvem PostSignum QCA.

Kvalifikované systémové certifikáty veřejného klíče vydané podle této certifikační politiky jsou určeny pro autority vydávající kvalifikovaná časová razítka (dále i autority časového razítka nebo i TSA), které jsou provozovány v rámci hierarchie PostSignum České pošty.

Autorita časového razítka, které byl vydán certifikát podle této certifikační politiky, musí být provozována Českou poštou

**Certifikáty vydané podle této certifikační politiky mohou být použity pouze pro ověření elektronické značky kvalifikovaného časového razítka v souladu se [ZoEP] a [Z300].**

Soukromý klíč odpovídající veřejnému klíči v certifikátu vydaném podle této certifikační politiky je určen k vytvoření elektronické značky na kvalifikovaném časovém razítku.

Plnění zásad této politiky rozpracovává a zajišťuje aktuální Certifikační prováděcí směrnice PostSignum QCA.

## 1.2 Název a jednoznačné určení dokumentu

**Tabulka 1: Identifikace politiky**

| | |
|---|---|
| Název dokumentu | Certifikační politika PostSignum Qualified CA pro certifikáty TSA |
| Verze dokumentu | 1.4 |
| Stav | finální |
| OID poskytovatele certifikačních služeb | 2.23.134 |
| OID PostSignum Root QCA | 2.23.134.1.4.2.1 |
| OID PostSignum Qualified CA | 2.23.134.1.4.2.2 |
| OID této politiky | 2.23.134.1.4.1.101.140 |
| Datum vydání | 1. 3. 2014 |
| Doba platnosti | Do odvolání nebo do dne ukončení služeb autorit PostSignum QCA. |

## 1.3 Participující subjekty

Podřízené certifikační autority mohou být řízeny a provozovány pouze Českou poštou (s výjimkou registračních autorit - viz dále).

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.: 267 196 111

e-mail: info@cpost.cz

Česká pošta je akreditovaným poskytovatelem certifikačních služeb na základě akreditace udělené Ministerstvem informatiky ČR dne 3.8.2005.

1.3.1 Certifikační autority (dále „CA“)

Úkolem CA PostSignum QCA je především vydávat a spravovat certifikáty certifikačních autorit PostSignum Root QCA, PostSignum Qualified CA a zákazníků České pošty v souladu s definovanými certifikačními politikami.

1.3.2 Registrační autority (dále „RA“)

Služby registračních autorit jsou zajišťovány poskytovatelem certifikačních služeb nebo externím subjektem na základě smlouvy s Českou poštou jako poskytovatelem certifikačních služeb.

Registrační autority zajišťují zejména tyto služby:

- přijímají (registrují) žádosti o certifikát, schvalují je nebo zamítají v souladu s platnými certifikačními politikami,
- ověřují totožnost žadatelů o certifikát,
- zajišťují předání vydaného certifikátu žadateli,
- zneplatňují certifikáty podle platných certifikačních politik.

Kontaktní údaje registračních autorit České pošty jsou uvedeny na webových stránkách poskytovatele.

Registrační autority zajišťované externím subjektem mohou poskytovat jen vybrané služby z výše uvedeného seznamu, což je stanoveno ve smlouvě mezi externím subjektem a Českou poštou.

V případě certifikátů pro ověření elektronické značky kvalifikovaného časového razítka žadatel o certifikát služby registračních autorit nevyužívá.

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

Držitelem kvalifikovaného systémového certifikátu vydaného podle této certifikační politiky je organizace Česká pošta.

Pro účely této politiky je držitel zastoupen osobou odpovědnou za poskytování služby vydávání kvalifikovaných časových razítek, konkrétně osobou v roli Manažer CA. V roli žadatele o certifikát vystupuje Administrátor systému CA.

1.3.4 Spoléhající se strany

Spoléhající se stranou je libovolný subjekt spoléhající se na certifikát vydaný PostSignum QCA. Spoléhající se strany nevstupují do smluvního vztahu s poskytovatelem certifikačních služeb.

1.3.5 Jiné participující subjekty

Certifikační autorita PostSignum QCA může využívat pro zajištění poskytování služeb externí subjekty.

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

Kvalifikované certifikáty vydané podle této certifikační politiky mohou být použity pouze pro ověření elektronické značky kvalifikovaného časového razítka v souladu se [ZoEP] a [Z300].

1.4.2 Omezení použití certifikátu

Kvalifikované certifikáty vydávané podle této certifikační politiky nejsou primárně určené pro komunikace nebo transakce v oblastech se zvýšeným rizikem škod na zdraví nebo na majetku, jako jsou chemické provozy, letecký provoz, provoz jaderných zařízení apod. nebo v souvislosti s bezpečností a obranyschopností státu. Česká pošta je připravena diskutovat se zákazníkem zvláštní podmínky poskytování certifikačních služeb ve výše uvedených sektorech.

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

1.5.1 Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

Za správu této certifikační politiky je odpovědný poskytovatel certifikačních služeb, tedy Česká pošta, konkrétně Manažer CA.

1.5.2 Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

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

manager.postsignum@cpost.cz,

nebo na webových stránkách poskytovatele.

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

Za správu této certifikační politiky odpovídá Manažer CA, 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, který je dle potřeby ustavován Komisí pro certifikační politiky ČP, je jí řízen a kontrolován.

Vypracovanou politiku předloží Manažer CA ke schválení Komisi pro certifikační politiky, která potvrdí OID politiky a přidělí číslo verze.

## 1.6 Přehled použitých pojmů a zkratek

**CDP (CRL Distribution Point)** – URL adresa uvedená v certifikátu, ze které lze stáhnout aktuální CRL.

**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 certifikační politiky a certifikační prováděcí směrnice, jimiž se řídí činnost certifikační autority.

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

**Kvalifikovaný certifikát** – kvalifikovaný certifikát ve smyslu [ZoEP].

**Kvalifikovaný systémový certifikát** – kvalifikovaný systémový certifikát ve smyslu [ZoEP].

**Kvalifikované časové razítko** – kvalifikované časové razítko ve smyslu [ZoEP].

**Manažer CA** – osoba v řídící roli zodpovědná za provoz PostSignum QCA a PostSignum VCA.

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

**Následný certifikát** – certifikát vydaný na základě uzavřené smlouvy jako náhrada za již vydaný certifikát PostSignum; příslušná certifikační politika stanovuje, které údaje původního certifikátu mohou být v následném certifikátu změněny. Pro vydání následného certifikátu není vyžadovaná fyzická návštěva registrační autority.

**Obchodní místo** – centrální regionální pracoviště poskytující certifikační služby a zajišťující evidenci smluv.

**Ověřovací registrační autorita** – zajišťuje vybrané služby registrační autority.

**Online Certificate Status Protocol (OCSP)** – protokol pro on-line zjištění stavu (zneplatnění) certifikátu.

**Otisk** – unikátní datový řetězec o neměnné délce, který je vypočítán z libovolných vstupních dat; jednoznačně reprezentuje vstupní data, tj. neexistuje stejný otisk pro dvě různé zprávy.

**Označující osoba** – osoba definovaná [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.

**Podepisující osoba** – osoba definovaná [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 [ZoEP].

**PostSignum VCA** – hierarchie certifikačních autorit, vydávajících komerční certifikáty.

**PostSignum Root QCA** – kořenová certifikační autorita, která má samopodepsaný kvalifikovaný systémový certifikát. Vydává kvalifikované systémové certifikáty pro podřízené certifikační autority a CRL. V hierarchii PostSignum mohou existovat další kořenové certifikační autority, které jsou navíc označeny pořadovým číslem, např. PostSignum Root QCA 2.

**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. V hierarchii PostSignum QCA mohou existovat další podřízené certifikační autority, které jsou navíc označeny pořadovým číslem, např. PostSignum Qualified CA 2.

**PostSignum Public CA** – certifikační autorita, která má kvalifikovaný systémový certifikát podepsaný kořenovou certifikační autoritou PostSignum Root QCA. Vydává komerční certifikáty pro subjekty, které nejsou certifikačními autoritami. V hierarchii PostSignum VCA mohou existovat další podřízené certifikační autority, které jsou navíc označeny pořadovým číslem, např. PostSignum Public CA 2.

**PostSignum TSA** – autorita vydávající kvalifikovaná časová razítka ve smyslu [ZoEP]. Autoritu tvoří více jednotek (TSU). Každá jednotka má vlastní klíč a kvalifikovaný systémový certifikát.

**Pověřená osoba** – ten, kdo vůči certifikační autoritě vystupuje jako zástupce zákazníka. Pověřené osoby musí být vyjmenovány ve smlouvě mezi zákazníkem a Českou poštou, případně smlouva stanovuje, že se jedná o samotného zákazníka.

**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, dat pro vytváření elektronických značek, dat pro šifrování a dešifrování a dat pro autentizaci.

**Správa žadatelů** – aplikace 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 například pro ověření elektronického podpisu či značky nebo pro zajištění jiných bezpečnostních služeb. Jinak též označována jako Osoba spoléhající se na certifikát.

**VCA ČP –** viz PostSignum VCA.

**Veřejný klíč** – souhrnné označení dat pro ověřování elektronického podpisu, dat pro ověřování elektronických značek a dat pro šifrování.

**Webové stránky poskytovatele** – http://www.postsignum.cz – webové stránky poskytovatele služby PostSignum.

**Zákazník** – nepodnikající fyzická osoba, podnikající fyzická osoba, právnická osoba, státní orgán nebo orgán místní samosprávy. Uzavírá s Českou poštou smlouvu o poskytování certifikačních služeb.

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

**Zákazník – podnikající fyzická osoba** – podnikající osoba s přiřazeným identifikačním číslem bez zaměstnanců.

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

**Zaměstnanec –** osoba v zaměstnaneckém nebo jiném poměru k zákazníkovi, pro kterou zákazník schválil vydání certifikátu podle této certifikační politiky.

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

Za zveřejňování informací odpovídá Česká pošta 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 jsou zveřejňovány:

- na webových stránkách poskytovatele

  www.postsignum.cz,

  postsignum.ttc.cz, nebo

- na obchodních místech České pošty, kde je možné požádat o jejich zkopírování na přinesené médium.

Vydané certifikáty koncových uživatelů (a s nimi spojené informace), u nichž zákazník (držitel certifikátu) souhlasil se zveřejněním, jsou zveřejňovány

- na webových stránkách poskytovatele.

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

- na webových stránkách poskytovatele, nebo
- na distribučních bodech seznamu zneplatněných certifikátů uvedených ve vydaném certifikátu (CDP).

### 2.2.2 Zveřejňování informací o certifikační autoritě

Certifikační politiky, zpráva pro uživatele a případně i další dokumenty jsou zveřejňovány

- na webových stránkách poskytovatele, nebo
- na obchodních místech (pouze k nahlédnutí).

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

- na webových stránkách poskytovatele,
- na obchodních místech a registračních autoritách ve formě vyvěšeného textového oznámení,
- 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 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 dva pracovní dny před zahájením označování časových razítek s využitím soukromých klíčů spojených s vydanými certifikáty;
- informace o stavu certifikátu ve formě seznamu zneplatněných certifikátů (CRL) jsou zveřejňovány neprodleně po jejich vydání, nejpozději však před koncem platnosti posledního zveřejněného seznamu zneplatněných certifikátů;
- 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.

Poskytovatel certifikačních služeb neumožňuje neautorizovaný přístup k vydaným certifikátům, u kterých nebyl držitelem vysloven souhlas se zveřejněním.

# 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 atributech subjektu certifikátu a v rozšířeních certifikátu je popsán v kapitole 7.

### 3.1.3 Anonymita a používání pseudonymu

PostSignum Qualified CA nepodporuje pseudonym žadatele o certifikát ani zákazníka v položce Subject certifikátu.

### 3.1.4 Pravidla pro interpretaci různých forem jmen

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

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

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

### 3.1.5 Jedinečnost jmen

PostSignum QCA si vyhrazuje právo upravit označení držitele certifikátu vydaného podle této certifikační politiky (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, která PostSignum QCA ověřuje, mají předepsanou strukturu a musí být doložena jejich správnost a úplnost (viz ustanovení kapitoly 3.2.2).

Odpovědnost za použití obchodních značek nebo registrovaných ochranných známek v polích certifikátu, které nejsou PostSignum QCA ověřovány (viz kapitola 3.2.2), má držitel certifikátu.

## 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 certifikační autoritě elektronickou žádost ve formátu PKCS#10 obsahující veřejný klíč, která je označena 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 se vydávají pro autority vydávající kvalifikovaná časová razítka, jejichž provozovatelem je Česká pošta.

Oprávněným žadatelem o certifikát autority časového razítka je příslušný zaměstnanec České pošty v roli Administrátor systému CA. Svou totožnost a své oprávnění dokládá podle vnitřních předpisů České pošty.

3.2.3 Ověřování identity fyzické osoby

Viz ustanovení v kapitole 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 autority časového razítka jsou náležitým způsobem ověřeny.

3.2.5 Ověřování specifických práv

Žádná ustanovení v této kapitole.

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 touto 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 kapitole 3.2.

3.3.2 Identifikace a autentizace při výměně párových dat po zneplatnění certifikátu

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

3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu

Oprávněným žadatelem o zneplatnění certifikátu autority časových razítek je Manažer CA. Svou totožnost a své oprávnění dokládá podle vnitřních předpisů České pošty.

O zneplatnění kvalifikovaného certifikátu může požádat ministerstvo podle [V378]. Oprávněným žadatelem o zneplatnění kvalifikovaného certifikátu je v tomto případě zástupce ministerstva.

# 4 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

## 4.1 Žádost o vydání certifikátu

### 4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu

Certifikáty podle této politiky jsou vydávány pro autority časového razítka vydávající kvalifikovaná časová razítka ve smyslu [ZoEP], jejichž provozovatelem je Česká pošta. Oprávněným žadatelem o certifikát autority časového razítka je Administrátor systému CA.

### 4.1.2 Registrační proces a odpovědnosti poskytovatele a žadatele

Písemná žádost o vydání certifikátu TSA je předkládána Manažerovi CA Žádost musí obsahovat následující identifikační údaje TSA, pro kterou má být vydán certifikát:

- jméno TSA,
- provozovatel TSA – konkrétní jméno odboru České pošty.

Žádost musí být podepsána zástupcem TSA oprávněným k podání žádosti.

K žádosti musí být přiloženy tyto dokumenty (nebo v případě jejich obecné dostupnosti odkazy na tyto dokumenty):

- prováděcí směrnice TSA,
- systémová bezpečnostní politika TSA.

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

#### 4.1.2.1 Odpovědnost žadatele resp. držitele certifikátu

Žadatel resp. držitel certifikátu TSA 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, na webových stránkách poskytovatele, případně jinými vhodnými způsoby (viz kapitola 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 kapitoly 3.2.2.

4.2.2 Přijetí nebo zamítnutí žádosti o certifikát

Manažer CA na základě předložené žádosti rozhodne, zda bude pro danou TSA vydán certifikát.

4.2.3 Doba zpracování žádosti o certifikát

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

4.3 Vydání certifikátu

Po kontrole žádosti o certifikát vloží obsluha certifikační autority (Architekt UniCERT) tuto žádost do systému certifikační autority, schválí ji a tím ji odešle ke zpracování. Systém certifikační autority na základě této žádosti vydá certifikát a předá ho zpět obsluze a případně i publikačním službám.

Certifikát se stává platným okamžikem vydání.

4.3.1 Úkony CA v průběhu vydávání certifikátu

Po schválení písemné žádosti předá zástupce TSA obsluze certifikační autority 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 TSA obsluze certifikační autority druhou písemnou žádost obsahující následující údaje:

- jméno TSA,
- provozovatel TSA – konkrétní jméno odboru České pošty,
- otisk („fingerprint“) veřejného klíče TSA a označení použitého algoritmu pro výpočet otisku.

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 TSA je zástupci TSA předán ve formátu DER spolu s certifikátem PostSignum Root QCA a PostSignum Qualified CA. Žadatel o certifikát nebo jeho zplnomocněný zástupce osobně přebírá certifikát a kontroluje, zda jsou údaje uvedené v certifikátu v pořádku. Pokud údaje souhlasí, zástupce TSA 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 budoucí držitel certifikátu (tedy Česká pošta) stvrzuje:

- že na sebe bere závazky vyplývající z této certifikační politiky,
- 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 této certifikační politice,
- že údaje ve vydaném certifikátu jsou správné a úplné.

Převzetím certifikátu se Česká pošta stává držitelem certifikátu.

4.4.2 Zveřejňování vydaných certifikátů poskytovatelem

Certifikáty vydané PostSignum Qualified CA pro ověřování elektronických značek pro ověření kvalifikovaných časových razítek jsou zveřejňovány elektronickou cestou nejpozději dva pracovní dny před zahájením označování časových razítek s využitím soukromých klíčů spojených s vydanými certifikáty.

4.4.3 Oznámení o vydání certifikátu jiným subjektům

Vydání certifikátu dle této certifikační politiky je oznámeno orgánu dle [ZoEP] a vydaný certifikát je předán orgánu ke kontrole.

Toto ustanovení se netýká předávání seznamu všech vydaných kvalifikovaných certifikátů na základě žádosti ministerstva podle [V378].

4.5 Použití párových dat a certifikátu

Platnost certifikátu vydaného podle této politiky je uvedena ve vydaném certifikátu.

Platnost párových dat pro označování časových razítek (soukromých a veřejných klíčů) jednotek TSU je omezena na dobu platnosti certifikátu TSA. Toto období je rozděleno do dvou časových úseků:

- prvního časového úseku, který trvá zpravidla 1 rok, kdy jsou párová data používána jak k vydávání časových razítek (používán soukromý klíč), tak i ověřování elektronické značky (používán veřejný klíč) a
- navazujícího časového úseku, kdy jsou data používána výhradně pro ověřování elektronické značky (používán veřejný klíč).

Celková platnost párových dat je ukončena v okamžiku uvedeném v certifikátu obsahujícím veřejný klíč z párových dat, nebo zneplatněním certifikátu s důvodem zneplatnění keyCompromise (1), caCompromise (2) nebo bez uvedeného důvodu pro zneplatnění.

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 (tj. provozovatel TSA):

- nakládá 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 informuje poskytovatele certifikačních služeb a zároveň ukončí používání uvedeného soukromého klíče,
- užívá soukromý klíč a odpovídající certifikát vydaný podle této certifikační politiky pouze pro účely stanovené v této certifikační politice v kapitole 1.4.1, tj. pro vytváření elektronické značky označující kvalifikované časové razítko v souladu s požadavky [ZoEP].

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

Uživatel certifikátu (spoléhající se strana) vydaného PostSignum Qualified CA:

- získá certifikáty PostSignum Qualified CA a PostSignum Root QCA z bezpečného zdroje (webové stránky poskytovatele, webové stránky ministerstva podle [V378], na pracovišti registrační autority) a ověří otisk ("fingerprint") těchto certifikátů;
- před použitím certifikátu vydaného PostSignum Qualified CA ověří platnost certifikátu PostSignum Qualified CA a následně i platnost vydaného koncového certifikátu; kontrola se provádí na správnost

podpisu vydávající autority a vůči příslušnému aktuálnímu CRL a aktuálnímu času (tuto činnost obvykle vykonává aplikace uživatele certifikátu);

- dostatečně zváží, zda je certifikát vydaný podle této politiky vhodný pro účel, ke kterému jej chce použít.

4.6 Obnovení certifikátu

Pod službou obnovení certifikátu je myšleno vydání nového certifikátu se stejným veřejným klíčem a novou dobou platnosti. PostSignum QCA tuto službu neposkytuje.

4.6.1 Podmínky pro obnovení certifikátu

PostSignum QCA tuto službu neposkytuje.

4.6.2 Subjekty oprávněné požadovat obnovení certifikátu

PostSignum QCA tuto službu neposkytuje.

4.6.3 Zpracování požadavku na obnovení certifikátu

PostSignum QCA tuto službu neposkytuje.

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

PostSignum QCA tuto službu neposkytuje.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu

PostSignum QCA tuto službu neposkytuje.

4.6.6 Zveřejňování vydaných obnovených certifikátů poskytovatelem

PostSignum QCA tuto službu neposkytuje.

4.6.7 Oznámení o vydání obnoveného certifikátu jiným subjektům

PostSignum QCA tuto službu neposkytuje.

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 (viz kapitola 4.1); není nutné měnit subjekt certifikátu autority časového razítka.

V tomto případě je nutné k žádosti přikládat pouze ty dokumenty, které byly od posledního vydání certifikátu změněny.

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

Viz ustanovení kapitoly 4.7.

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

Viz ustanovení kapitoly 4.7.

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

Viz ustanovení kapitoly 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 kapitoly 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 kapitoly 4.7.

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

Viz ustanovení kapitoly 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 kapitoly 4.7.

4.8 Změna údajů v certifikátu

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

4.8.1 Podmínky pro změnu údajů v certifikátu

Viz ustanovení kapitoly 4.8.

4.8.2 Subjekty oprávněné požadovat změnu údajů v certifikátu

Viz ustanovení kapitoly 4.8.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

Viz ustanovení kapitoly 4.8.

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

Viz ustanovení kapitoly 4.8.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Viz ustanovení kapitoly 4.8.

4.8.6 Zveřejňování vydaných certifikátů se změněnými údaji

Viz ustanovení kapitoly 4.8.

4.8.7 Oznámení o vydání certifikátu se změněnými údaji jiným subjektům

Viz ustanovení kapitoly 4.8.

4.9 Zneplatnění a pozastavení platnosti certifikátu

Důvody pro zneplatnění certifikátů vydaných podle této politiky je možné rozdělit do dvou skupin, které se následně liší možností použití certifikátu po času zneplatnění uvedeném na CRL:

V případě zneplatnění certifikátu s důvodem zneplatnění

- unspecified (0),
- affiliationChanged (3),
- superseded (4) nebo
- cessationOfOperation (5)

je možné certifikát používat k ověření elektronické značky na časových razítkách vydaných před časem zneplatnění certifikátu. Všechna časová razítka vydaná po tomto čase a označená soukromým klíčem odpovídajícím veřejnému klíči obsaženém v zneplatněném certifikátu je nutné považovat za neplatná.

V případě zneplatnění certifikátu s důvodem zneplatnění

- keyCompromise (1),
- caCompromise (2) nebo
- bez uvedeného důvodu pro zneplatnění

není možné certifikát používat k ověření elektronické značky na časových razítkách. Všechna časová razítka označená soukromým klíčem odpovídajícím veřejnému klíči, obsaženém ve zneplatněném certifikátu, je nutné považovat za neplatná.

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 je archivován v souladu s platnou legislativou a archivačními předpisy České pošty.

4.9.1 Podmínky pro zneplatnění certifikátu

Certifikát může být zneplatněn v případě jakékoliv podezření na kompromitaci odpovídajícího soukromého klíče, z vůle držitele certifikátu, z vůle poskytovatele certifikačních služeb nebo na základě nařízení ministerstva podle [V378].

4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

O zneplatnění certifikátu může požádat držitel certifikátu prostřednictvím Manažera CA, Manažer CA nebo zástupce ministerstva podle [V378].

4.9.3 Požadavek na zneplatnění certifikátu

4.9.3.1 Žádost o zneplatnění certifikátu podaná na žádost držitele certifikátu

O zneplatnění certifikátu TSA žádá Manažer CA písemně. V žádosti o zneplatnění musí být uveden důvod zneplatnění.

4.9.3.2 Žádost o zneplatnění certifikátu z vůle PostSignum QCA

Poskytovatel certifikačních služeb může zneplatnit certifikát držitele, který provozuje TSA 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 TSA.

Manažer CA podává písemnou žádost o zneplatnění certifikátu TSA, kterou předá některému z operátorů oprávněných provádět zneplatnění certifikátu. Po úspěšném zneplatnění certifikátu TSA je vytvořen protokol o zneplatnění certifikátu, který je neprodleně zaslán Manažerovi CA.

4.9.3.3 Zneplatnění certifikátu z vůle ministerstva podle [V378]

O zneplatnění kvalifikovaného certifikátu může rozhodnout rovněž ministerstvo podle [V378]. Zástupce ministerstva podává písemnou žádost o zneplatnění certifikátu Manažerovi CA, v žádosti musí být uveden důvod zneplatnění certifikátu.

Po úspěšném zneplatnění certifikátu TSA je vytvořen protokol o zneplatnění certifikátu, který je neprodleně zaslán Manažerovi CA.

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

Doba od přijetí žádosti o zneplatnění certifikátu do zveřejnění CRL obsahujícího i zneplatněný certifikát nepřesáhne 24 hodin.

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

Uživatel certifikátu vydaného PostSignum Qualified CA (spoléhající se strana) je povinen postupovat v souladu s ustanoveními kapitoly 4.5.2.

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů (CRL) je vydáván vždy vzápětí po zpracování žádosti o revokaci certifikátu. Nedojde-li k revokaci certifikátu, je nový CRL vydáván alespoň každých 24 hodin. Seznam zneplatněných certifikátů je zveřejňován na těchto místech:

- distribučních bodech CRL (CDP) uvedených v certifikátu
- na webových stránkách poskytovatele,
- u nezávislého poskytovatele webových služeb.

Primárním zdrojem aktuálního CRL jsou distribuční body CRL.

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

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

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

Certifikáty vydané dle této politiky je možné ověřit pomocí veřejně dostupné služby OCSP provozované PostSignum QCA.

URL adresa OCSP služby je:

http(s)://ocsp.postsignum.cz/OCSP/QCA2/OCSP_public/

4.9.10 Požadavky při ověřování statutu certifikátu on-line

Pro ověření certifikátu vydaného dle této certifikační politiky je možné využít veřejně dostupnou službu OCSP. OCSP služba je poskytována dle standardu RFC 2560. Formát žádosti a odpovědi OCSP je uveden v kapitole 7.3.

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,
- v rámci služby vyhledávání vydaných certifikátů přístupné na webových stránkách poskytovatele, nebo

- pomocí služby OCSP.

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 místech uvedených v kapitole 4.9.7.

V rámci služby vyhledávání vydaných certifikátů přístupné na webových stránkách poskytovatele je zveřejňována rovněž informace o stavu vyhledávaného certifikátu. Tato informace o stavu certifikátu je pouze informativní, jedná se pouze o doplňkovou informaci k aktuálnímu CRL, které je vždy závazným zdrojem informací o stavu certifikátu.

Služba OCSP vrací stav certifikátu v reálném čase (on-line) na základě zaslané žádosti, která musí splňovat náležitosti uvedené v kapitole 7.3. Odpověď OCSP serveru je podepsaná certifikátem OCSP serveru a má předepsaný formát, uvedený v kapitole 7.3. Informace o stavu certifikátu získané pomocí služby OCSP jsou závazným zdrojem informací o stavu certifikátu.

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.

Služba pro vyhledávání certifikátů je dostupná 7 dní v týdnu 24 hodin denně.

Veřejná služba OCSP je dostupná 7 dní v týdnu 24 hodin denně.

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 končí písemným oznámením ze strany Manažera CA. Toto se netýká služeb zneplatnění certifikátu, které jsou poskytovány po celou dobu platnosti certifikátu.

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 zvládání 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
- Organizační zajištění úlohy Kvalifikovaná certifikační autorita České pošty, 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

### 5.1.1 Umístění a konstrukce

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

- centrální pracoviště (hlavní a záložní lokalita),
- operátorská pracoviště centra (zejména pro správu podpůrného informačního systému),
- pracoviště registrační autority 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“.

Kromě toho existuje pracoviště mobilní registrační autority, kde je neexistence opatření z oblasti fyzické bezpečnosti kompenzována opatřeními z oblasti organizační bezpečnosti.

### 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. Na pracoviště mobilní registrační autority se vztahují režimová opatření definovaná v Systémové bezpečnostní politice.

5.1.3 Elektřina a klimatizace

Centrální pracoviště jsou připojena na nepřerušitelný zdroj napájení (UPS) a mají nainstalovánu 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.

5.1.5 Protipožární opatření a ochrana

Prostory centrálních pracovišť jsou vybaveny elektronickou požární signalizací (EPS).

5.1.6 Ukládání médií

Pro účely uskladnění dat PostSignum QCA jsou k dispozici trezory, minimálně jeden z nich je umístěn 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.

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 (bezpečným kryptografickým modulem) 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 používaná 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

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, 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 a mají dobré pracovní a osobní reference.

V případě, že daná osoba není zaměstnancem České pošty, 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.

O provedení školení musí být proveden písemný zápis obsahující mj. datum školení, obsah školení, jméno školitele a seznam účastníků. Tento zápis musí být podepsán všemi účastníky i školitelem.

U rolí určených Manažerem CA 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, 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 CA 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 nebo ustanoveními smlouvy mezi Českou poštou a smluvním partnerem.

5.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

Na smluvní (externí) pracovníky jsou uplatňována obdobná kriteria jako na zaměstnance České pošty.

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, zneplatnění 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 (kromě auditních záznamů o činnosti centrálních komponent certifikační autority v elektronické podobě) nejsou obecně zálohovány; jsou pouze archivovány. Důležité auditní záznamy spojené s vydáním certifikátů jsou uchovávány ve dvou kopiích, které jsou uložené v různých lokalitách.

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

V prostředí PostSignum QCA není nasazen systém na centrální shromažďování auditních záznamů. Auditní záznamy jsou 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 CA.

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 jsou archivovány 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

Pokud jsou v PostSignum QCA využívána časová razítka, jedná se o kvalifikovaná časová razítka PostSignum QCA.

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

V prostředí PostSignum QCA jsou auditní záznamy shromažďovány a přesouvány do Archivu CA 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.

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 popsaným v kapitole 2.

Nejméně 1 rok před vypršením platnosti certifikátu je provozovatel certifikační autority PostSignum Qualified CA povinen požádat o vydání dalšího certifikátu u PostSignum Root QCA.

Plánovaná výměna klíčů certifikační autority musí být oznámena zákazníkům nejpozději 6 měsíců před vydáním nového certifikátu PostSignum Root QCA resp. 3 měsíce před uskutečněním výměny certifikátu autority PostSignum Qualified CA. Toto oznámení bude (včetně důvodu ukončení platnosti certifikátu) zveřejněno na webových stránkách poskytovatele 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 parametry (např. velikostí modulu).

## 5.7 Obnova po havárii nebo kompromitaci

Pro PostSignum QCA byly vypracovány dokumenty popisující zvládání 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 zvládání 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 zvládání krizových situací a plán obnovy.

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

#### 5.7.3.1 Kompromitace soukromého klíče podřízené certifikační autority

V případě podezření na kompromitaci soukromého klíče PostSignum Qualified CA 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 poskytovatele, na všech pracovištích registrační autority PostSignum QCA a v jednom celostátně vydávaném deníku. Součástí oznámení bude i důvod ukončení platnosti certifikátu certifikační autority.

PostSignum Root QCA okamžitě zneplatní certifikát PostSignum Qualified CA a tato zneplatní všechny platné certifikáty vydané koncovým zákazníkům; zneplatněné certifikáty budou neprodleně zveřejněny na příslušném CRL.

Po zveřejnění informace o mimořádném ukončení činnosti končí platnost všech certifikátů vydaných PostSignum Qualified CA.

Česká pošta prokazatelně zničí data pro vytváření elektronických značek PostSignum Qualified CA, 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 nepopiratelně zpochybní důvěryhodnost vydávaných certifikátů a seznamů vydávaných certifikátů.

#### 5.7.3.2 Kompromitace soukromého klíče PostSignum Root QCA

V případě podezření na kompromitaci soukromého klíče PostSignum Root QCA 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. O zneplatnění certifikátů (případně o mimořádném

ukončení činnosti autority) budou písemně nebo elektronicky informováni všichni držitelé certifikátů, orgán určený [ZoEP, V378] a subjekty, které mají uzavřenou smlouvu přímo se vztahující k poskytování certifikačních služeb; oznámení bude rovněž zveřejněno na webových stránkách poskytovatele, na všech pracovištích registrační autority PostSignum QCA a v jednom celostátně vydávaném deníku. Součástí oznámení bude i důvod ukončení platnosti certifikátu certifikační autority.

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 nepopiratelně zpochybní důvěryhodnost vydávaných certifikátů a seznamů vydávaných certifikátů.

### 5.7.4 Schopnost obnovit činnost po havárii

Obnova činnosti po havárii se řídí platným interním dokumentem Plán zvládání krizových situací a plán obnovy.

## 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 poskytovatele 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 podřízené certifikační autority

Ukončení činnosti PostSignum Qualified CA 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 poskytovatele a na všech

pracovištích registrační autority PostSignum QCA. Součástí oznámení musí být i informace o ukončení platnosti certifikátu autority včetně příslušného důvodu ukončení. Dokud je platný alespoň jeden certifikát vydaný PostSignum Qualified CA, musí tato autorita zajišťovat alespoň funkci zneplatnění certifikátu a vydání CRL.

Pokud PostSignum Qualified CA 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 3 měsíce ode dne zaslání oznámení. K tomuto datu PostSignum Qualified CA zneplatní všechny dosud platné vydané certifikáty a vydá poslední CRL. Teprve poté může být činnost této autority ukončena.

Zneplatněný kvalifikovaný systémový certifikát PostSignum Qualified CA bude zveřejněn na CRL PostSignum Root QCA v čase uvedeném v certifikační politice PostSignum Root QCA.

Smlouvy o poskytování certifikačních služeb budou v tomto případě ukončeny ze strany ČP dohodou nebo výpovědí.

Následně ČP prokazatelně zničí data pro vytváření elektronických značek PostSignum Qualified CA, která sloužila pro podepisování 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.

### 5.8.3 Ukončení činnosti registrační autority

Ukončení činnosti pracoviště registrační autority je zákazníkům oznámeno vývěskami na příslušném pracovišti nebo na budově a na webových stránkách poskytovatele. Spolu s oznámením o ukončení činnosti pracoviště je uvedena i adresa a kontakty pracoviště náhradního.

### 5.8.4 Ukončení činnosti poskytovatele certifikačních služeb

Činnost poskytovatele certifikačních služeb bude ukončena v souladu s §13 [ZoEP].

### 5.8.5 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 poskytovatele, na všech pracovištích registrační autority PostSignum QCA a dalšími způsoby uvedenými v § 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 ministerstva podle [V378].

# 6 TECHNICKÁ BEZPEČNOST

## 6.1 Generování a instalace párových dat

Soukromé klíče žadatelů o certifikáty vydávané podle této certifikační politiky jsou generovány a uschovávány žadatelem o certifikát. Klíče musí být generovány a uloženy v hardwarovém kryptografickém modulu splňujícím požadavky [V378] pro uložení soukromých klíčů autority časového razítka. Musí se jednat o klíče pro algoritmus RSA, s délkou modulu 2048 bitů.

### 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 CA a Auditor CA.

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 a dále certifikáty podepisujících nebo označujících osob, pro které byl vysloven souhlas se zveřejněním, jsou zveřejněny způsobem popsaným v kapitole 2.2.1.

### 6.1.5 Délky párových dat

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

Klíče držitelů certifikátů vydaných podle této politiky mají pro algoritmus RSA délku modulu 2048 bitů. Jiný algoritmus než RSA není pro držitele certifikátů povolen.

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].

Parametry používané při vytváření veřejných klíčů žadatelů o certifikát jsou generovány softwarovým nebo hardwarovým vybavením žadatele.

Kontrola kvality dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek je nastavena na úrovni certifikační autority, která kontroluje jedinečnost a povolenou délku veřejného klíče.

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

Veřejné klíče koncových uživatelů 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 QCA 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 (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.

6.2.3 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. 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 QCA nejsou archivovány. Po ukončení provozu certifikační autority jsou klíče včetně záloh zničeny, o čemž je vyhotoven záznam.

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 interních dokumentů Systémová bezpečnostní politika, Provozní a bezpečnostní procedury a Auditní a archivační politika).

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

Klíč je do nového nebo inicializovaného kryptografického modulu vkládán ze 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 s interními dokumenty Systémovou bezpečnostní politikou a Provozními a bezpečnostními procedurami.

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 s interními dokumenty 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 kryptografickém modulu je zničen prostředky poskytovanými kryptografickým modulem v případě, že kryptografický modul má být dočasně použit k jiným účelům, v případě ukončení činnosti kryptografického modulu nebo v případě ukončení činnosti certifikační autority, jejíž klíče jsou v kryptografickém modulu uloženy. Toto zničení soukromého klíče se provádí autorizovanou obsluhou v souladu s ustanoveními interních dokumentů Systémová bezpečnostní politika a Provozní a bezpečnostní procedury nebo na základě požadavku Manažera CA.

Zničení soukromého klíče je provedeno uvedením kryptografického modulu do inicializovaného stavu, kdy je pomocí mechanismů kryptografického modulu bezpečně vymazán veškerý kryptografický materiál (včetně soukromého klíče CA). Zničení soukromého klíče zahrnuje i smazání všech 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 konstrukce 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 koncových uživatelů jsou archivovány v souladu s interním dokumentem Auditní a archivační politika.

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

Doba platnosti certifikátu vydaného podle této certifikační politiky je uvedena v certifikátu.

Doba platnosti soukromých klíčů svázaných s certifikáty vydanými podle této politiky je buď shodná s dobou platnosti certifikátu, nebo může být za předpokladu splnění ustanovení uvedených v kapitole 4.5 omezena.

## 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 interních dokumentech Systémové bezpečnostní politika, Provozní a bezpečnostní procedury a v interní provozní dokumentaci.

### 6.4.1 Generování a instalace aktivačních dat

Aktivační data jsou 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 prozrazením neoprávněné osobě. Příslušné povinnosti v tomto smyslu mají všichni pracovníci PostSignum QCA a jsou uvedeny v interním dokumentu Systémová bezpečnostní politika.

### 6.4.3 Ostatní aspekty aktivačních dat

Ostatní aspekty týkající se aktivačních dat, jejich generování, instalace a používání, jsou popsány v interních dokumentech Systémové bezpečnostní politika, Provozní a bezpečnostní procedury a v interní 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, která vycházejí z požadavků [V378] a návazných dokumentů, a to zejména ze standardů [CWA 141671] a [TS 101456].

### 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], [CWA 141671] a [TS 101456].

## 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 27001], 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

Lokální sítě centrálních pracovišť (hlavní a záložní lokalita) obsahující centrální systémy PostSignum QCA jsou od interní sítě ČP odděleny firewallem. Tento firewall neumožňuje žádnou komunikaci směrem z interní sítě ČP přímo do lokální sítě obsahující systémy PostSignum QCA. Veškerá komunikace směrem do lokální sítě centrálního pracoviště je ukončena na vyhrazené DMZ síti.

Interní síť ČP je mimo to od všech externích sítí včetně Internetu oddělena vlastním firewallem.

Veškerá komunikace mimo vyhrazené lokální sítě centrálních pracovišť je šifrovaná.

## 6.8 Časová razítka

Viz kapitola 5.5.5.

# 7 PROFILY CERTIFIKÁTU, SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ A OCSP

## 7.1 Profil certifikátu

PostSignum QCA vydává certifikáty odpovídající standardu X.509. Profil certifikátu TSA je uveden v následující tabulce.

**Tabulka 2: Profil certifikátu TSA**

| Název položky | Hodnota/příznak použití |
|---|---|
| **Version** | 3 (0x2) |
| **Serial Number** | *jednoznačné číslo certifikátu přidělené PostSignum Qualified CA* |
| **SignatureAlgorithm** | sha256WithRSAEncryption |
| **Issuer** | |
| Country | CZ |
| Organisation | Česká pošta, s.p. [IČ 47114983]<br>*uvedené číslo je IČ České pošty, s.p.* |
| CN | PostSignum Qualified CA X<br>*(X je číslo označující konkrétní podřízenou certifikační autoritu)* |
| **Validity** | |
| Not Before | Počátek platnosti vydaného certifikátu (UTCTime) |
| Not After | Konec platnosti vydaného certifikátu (UTCTime) |
| **Subject** | |
| Country | CZ |
| Organisation | Česká pošta, s.p. [IČ 47114983] |
| OU | Time Stamping Authority |
| CN | PostSignum TSA - TSU X<br>*X je číslo označující konkrétní jednotku TSU (X=1, 2, 3, 4, 5, 6)* |
| **Subject Public Key Info** | |
| Algorithm | rsaEncryption |
| SubjectPublicKey | *veřejný klíč TSU*<br>*algoritmus RSA, velikost klíče 2048 bitů* |
| **Extensions** | *rozšíření certifikátu podle tabulky 3* |
| **Signature** | *elektronická značka poskytovatele certifikačních služeb* |

### 7.1.1 Číslo verze

PostSignum Qualified CA vydává certifikáty vyhovující standardu X.509 verze 3.

### 7.1.2 Rozšiřující položky v certifikátu

Rozšiřující položky použité v certifikátu TSA jsou uvedeny v následující tabulce.

**Tabulka 3: Rozšíření v certifikátu TSA**

| Název rozšiřující položky | Hodnota/příznak použití | Kritická ano/ne |
|---|---|---|
| **Authority Key Identifier** | | ne |
| Key Identifier | *používá se* | |
| **Subject Key Identifier** | *používá se* | ne |
| **Key Usage** | | ano |
| DigitalSignature | ano | |
| NonRepudiation | ano | |
| KeyEncipherment | ne | |
| DataEncipherment | ne | |
| KeyAgreement | ne | |
| KeyCertSign | ne | |
| CRLSign | ne | |
| **Extended Key usage** | | ano |
| KeyPurposeID | id-kp-timeStamping | |
| **CertificatePolicies** | | ne |
| Policy Identifier | OID této certifikační politiky | |
| Policy Qualifier id | CPS | |
| CPS URI | http://www.postsignum.cz | |
| User Notice | Tento kvalifikovany systemovy certifikat byl vydan podle zakona 227/2000Sb. a navaznych predpisu/This qualified system certificate was issued according to Law No 227/2000Coll. and related regulations | |
| **Qualified certificate statement** | | ne |
| OID | 1.3.6.1.5.5.7.11.2 (PKIX QC Statements Extension id-qcs-pkixQCSyntax-v2) | |
| **CRL Distribution Points** | | ne |
| URI | http://www.postsignum.cz/crl/psqualifiedcaX.crl | |
| URI | http://www2.postsignum.cz/crl/psqualifiedcaX.crl | |
| URI | http://postsignum.ttc.cz/crl/psqualifiedcaX.crl | |
| *(X je číslo označující konkrétní podřízenou certifikační autoritu)* | | |
| **AuthorityInfoAccess** | | |
| accessMethod<br>URI | id-ad-caIssuers (1.3.6.1.5.5.7.48.2)<br>http://www.postsignum.cz/crt/psqualifiedcaX.crt | |
| accessMethod<br>URI | id-ad-caIssuers (1.3.6.1.5.5.7.48.2)<br>http://www2.postsignum.cz/crt/psqualifiedcaX.crt | |
| accessMethod<br>URI | id-ad-caIssuers (1.3.6.1.5.5.7.48.2)<br>http://postsignum.ttc.cz/crt/psqualifiedcaX.crt | |
| *(X je číslo označující konkrétní podřízenou certifikační autoritu)* | | |

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

### 7.1.3 Objektové identifikátory (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 kapitolách 3.1.1 až 3.1.4.

7.1.5 Omezení jmen a názvů

Certifikáty vydávané podle této certifikační politiky mohou obsahovat pouze jména a názvy uvedená v profilu certifikátu, uvedeném v kapitole 7.1.

7.1.6 OID certifikační politiky

V každém certifikátu koncového uživatele je uveden odkaz na politiku, podle které byl certifikát vydán. Tento odkaz je realizován uvedením OID politiky v certifikátu.

OID této politiky je uvedeno v kapitole 1.2.

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 odkaz na webové stránky poskytovatele, kde lze získat certifikační politiku, podle které byl certifikát vydán, a textovou informaci o skutečnosti, 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

**Tabulka 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 Qualified CA X<br>*(X je číslo označující konkrétní podřízenou certifikační autoritu)* |
| **Validity** | |
| This Update | Počátek platnosti vydaného CRL (UTCTime) |
| Next Update | Konec platnosti vydaného CRL (UTCTime) |
| **RevokedCertificates** | *opakující se položka pro každý zneplatněný certifikát* |
| UserCertificate | *sériové číslo zneplatněného certifikátu* |
| RevocationDate | *datum a čas zneplatnění* |
| CrlEntryExtensions | *rozšíření položky CRL podle tabulky 5* |
| **CrlExtensions** | *rozšíření CRL podle tabulky 5* |
| **SignatureAlgorithm** | sha256WithRSAEncryption |
| **Signature** | *elektronická značka poskytovatele certifikačních služeb* |

7.2.1 Číslo verze

PostSignum Qualified CA vydává seznamy zneplatněných certifikátů podle standardu X.509 verze 2.

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

**Tabulka 5: Rozšíření v CRL**

| Název rozšiřující položky | Hodnota/příznak použití | Kritická ano/ne |
|---|---|---|
| **Rozšíření položky CrlEntryExtensions** | | |
| InvalidityDate | datum a čas vzniku události vedoucí ke zneplatnění certifikátu; volitelné rozšíření | ne |
| ReasonCode | důvod zneplatnění certifikátu | ne |
| **Rozšíření pro CRL (CrlExtensions)** | | |
| Authority Key Identifier | | ne |
| Key Identifier | *používá se* | |
| AuthorityCertIssuer | *používá se* | |
| AuthorityCertSerialNumber | *používá se* | |
| CRL Number | *jednoznačné číslo CRL přidělené PostSignum Qualified CA* | ne |

## 7.3 Profil OCSP

**Tabulka 6: Struktura OCSP žádosti – OCSP Request Data**

| Název položky | Popis | Hodnota/příznak použití |
|---|---|---|
| Version | Verze protokolu OCSP (povinná položka) | 1 |
| Requestor List | | |
| Certificate ID | údaje o dotazovaném certifikátu – položka se může opakovat | |
| Hash Algorithm | hash žádosti | SHA-1 |
| Issuer Name Hash | hash vypočítaný ze jména vydavatele certifikátu | |
| Issuer Key Hash | hash vypočítaný z otisku veřejného klíče vydavatele certifikátu | |
| Serial Number | sériové číslo dotazovaného certifikátu | |
| Request Extensions | | |
| OCSP Nonce | Náhodné, jednou vygenerované číslo (64 bitů). Je-li obsaženo v žádosti, pak ho obsahuje i odpověď. (nepovinná položka) | |

Žádost OCSP nemusí být podepsaná.

**Tabulka 7: Struktura OCSP odpovědi – OCSP Response Data**

| Název položky | Popis | Hodnota/příznak použití |
|---|---|---|
| OCSP Response Status | Přirozené číslo, označující stav odpovědi | 0 – successful<br>1 – malformedRequest<br>2 – internalError<br>3 – tryLater<br>6 – unauthorized |
| Response Type | Basic OCSP Response | |
| Version | Verze protokolu OCSP | 1 |
| Responder Id | DN podpisového certifikátu OCSP serveru | |

| | | |
|---|---|---|
| Produced At | Čas podpisu odpovědi OCSP serveru | |
| Responses: | | |
| Certificate ID | Údaje odpovídají údajům v žádosti | |
| Cert Status | Stav certifikátu.<br>good – certifikát je platný<br>revoked – certifikát je zneplatněný<br>unknown – stav certifikátu je neznámý (např. takový certifikát neexistuje) | 0 – good<br>1 – revoked<br>2 – unknown |
| Revocation Time | Čas revokace certifikátu. Položka je uvedena pouze v případě Cert Status=revoked | |
| Revocation Reason | Důvod revokace certifikátu. Položka je uvedena pouze v případě Cert Status=revoked | |
| This Update | Čas, od něhož je indikován stav odpovědi. | |
| Response Extensions | | |
| OCSP Nonce | Náhodné, jednou vygenerované číslo (64 bitů). Je-li obsaženo v žádosti, pak ho obsahuje i odpověď. (nepovinná položka) | |

### 7.3.1 Číslo verze

Viz údaje v tabulkách 6 a 7.

### 7.3.2 Rozšiřující položky OCSP

Viz údaje v tabulkách 6 a 7.

# 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 CA, managementu České pošty nebo odboru interního auditu 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 dokumentaci QCA označováni jako Auditoři CA.

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, kteří se nepodílejí na provozu certifikační autority PostSignum QCA.

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

8.4 Hodnocené oblasti

Oblasti hodnocené v rámci pravidelných kontrol jsou specifikovány v [ZoEP], [V378] a příslušnými standardy, které jsou uvedeny v příloze [V378].

8.5 Postup v případě zjištění nedostatků

Výsledky kontrol jsou předávány Manažerovi CA, 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 CA. Ten zajistí její distribuci a projednání. Pokud je součástí zprávy zpráva o kontrole bezpečnostní shody ve smyslu §8, odst. 2 [V378], zajistí Manažer CA její předání ministerstvu podle [V378] do 30 dní od ukončení této kontroly bezpečnostní shody.

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

# 9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

## 9.1 Poplatky

### 9.1.1 Poplatky za vydání nebo obnovení certifikátu

Poplatky za vydávání certifikátů autorit časového razítka 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

Poplatky za případné další služby se neúčtují.

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

Žádná ustanovení v této kapitole.

## 9.2 Finanční odpovědnost

### 9.2.1 Krytí pojištěním

Česká pošta má sjednané pojištění odpovědnosti za škodu takovým způsobem, aby byly pokryty případné škody.

### 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.ceskaposta.cz).

### 9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

PostSignum QCA tuto službu neposkytuje.

## 9.3 Citlivost obchodních informací

V maximálním rozsahu podle ustanovení platných právních předpisů se každá ze zúčastněných stran zavazuje uchovat v tajnosti veškeré důvěrné informace, okolnosti a údaje, které se dozvěděla v souvislosti s plněním smlouvy o poskytování certifikačních služeb a o kterých nebylo písemně dohodnuto mezi smluvními stranami, že mohou být zveřejněny.

### 9.3.1 Výčet citlivých informací

Za důvěrné jsou považovány všechny informace s výjimkou informací uvedených v dokumentech s označením „Veřejné“.

9.3.2 Informace mimo rámec citlivých informací

Za důvěrné se nepovažují informace, které:

- se staly veřejně známými, aniž by to zavinila záměrně či opomenutím přijímající strana,
- měla přijímající strana legálně k dispozici před uzavřením smlouvy o poskytování certifikačních služeb, pokud takové informace nebyly předmětem jiné, dříve mezi zúčastněnými stranami uzavřené smlouvy o ochraně informací, nebo pokud takové informace nemají samy o sobě charakter obchodního tajemství,
- jsou výsledkem postupu, při kterém k nim přijímající strana dospěje nezávisle a je schopna to doložit svými záznamy nebo důvěrnými informacemi třetí strany,
- po uzavření smlouvy o poskytování certifikačních služeb poskytne přijímající straně třetí osoba, jež takové informace přitom nezíská přímo ani nepřímo od strany, jež je jejich vlastníkem, nebo je nezíská nezákonným způsobem, o čemž by přijímající strana věděla nebo vědět musela,
- jsou uvedené v kvalifikovaném systémovém certifikátu, pokud k jeho zveřejnění dal držitel souhlas.

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, [VOP] a v Certifikační prováděcí směrnici a vycházejí z příslušných ustanovení [Z101].

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 jsou obsaženy v certifikačních politikách, [VOP] a 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 (v případě této certifikační politiky zejména zástupce TSA).

9.4.3 Údaje, které nejsou považovány za citlivé

Za citlivé nejsou považovány informace, které nespadají pod ochranu [Z101], nebo které byly z rozhodnutí příslušné fyzické osoby určeny ke zveřejnění (certifikát, položky v certifikátu).

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 (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 CA 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 ustavení [Z101] a interních předpisů České pošty, 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 poskytovatele.

9.6 Zastupování a záruky

Česká pošta zaručuje, že splní veškeré povinnosti uložené touto certifikační politikou a 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 kapitoly 9.6.

9.6.2 Zastupování a záruky RA

V poskytování služeb registrační autority může být Česká pošta jako poskytovatel certifikačních služeb zastupována třetím subjektem na základě uzavřeného smluvního vztahu; uvedená úroveň záruk není tímto dotčena.

Jinak viz ustanovení kapitoly 9.6.

9.6.3 Zastupování a záruky držitele certifikátu, podepisující nebo označující osoby

Držitel certifikátu vydaného podle této certifikační politiky ručí za naplnění všech povinností zákazníků a žadatelů o certifikát uvedených v této certifikační politice a povinností uvedených v [ZoEP].

9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strana se zaručuje, že kvalifikovaný certifikát bude používat podle ustanovení v této certifikační politice, především v kapitole 4.5.2.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Subjekty, které se přímo podílí na provozu PostSignum QCA na základě smluvního vztahu s poskytovatelem certifikačních služeb, mají povinnost dodržovat ustanovení certifikační politiky, certifikační prováděcí směrnice, systémové bezpečnostní politiky a dalších interních dokumentů.

Záruky, které v těchto případech poskytuje poskytovatel certifikačních služeb, jsou definovány příslušnými ustanoveními [ZoEP] a [V378].

9.7 Zřeknutí se záruk

Záruky uvedené v kapitole 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 poskytnutých v rámci plnění smlouvy o poskytování certifikačních služeb držitelem, 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.

V případě, že provozovatelem TSA je Česká pošta, je náhrada způsobené škody řešena v souladu s interními předpisy České pošty.

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 webové stránce poskytovatele.

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

Česká pošta odpovídá za škodu podle platných právních předpisů.

9.10 Doba platnosti, ukončení platnosti

9.10.1 Doba platnosti

Doba platnosti této certifikační politiky je od data vydání uvedeného v kapitole 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, jakožto 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 zákazníkům, 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 popsanými v kapitole 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 kapitole 1.5.

9.12.2 Postup při oznamování změn

Vydání nové certifikační politiky se změněným OID (viz následující kapitola) bude oznámeno v aktualitách na webových stránkách poskytovatele.

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 poskytovatele, na všech pracovištích registrační autority PostSignum QCA. Na toto oznámení mohou navazovat další akce, které jsou popsány v této certifikační politice.

V případě, že nebude hrozit nebezpečí z prodlení, bude toto oznámení provedeno min. 10 pracovních dní před začátkem platnosti nové verze certifikační politiky.

9.12.3 Okolnosti, při kterých musí být změněn OID

Česká pošta 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 směrnici.

Jakákoliv změna v certifikační politice vyvolá změnu verze dokumentu i změnu OID.

## 9.13 Řešení sporů

Spory řeší věcně a místně příslušný soud.

## 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 [ZoEP] a [V378].

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 této kapitole.

### 9.16.2 Postoupení práv

Česká pošta může pro zajištění vykonávání svých činností využít služeb jiného právního subjektu, u kterého je zajištěna stejná úroveň bezpečnosti i poskytovaných služeb. Vztahy mezi Českou poštou a tímto subjektem budou upraveny zvláštní smlouvou. Povinnosti a odpovědnost České pošty, jakožto poskytovatele certifikačních služeb, zůstávají tímto nedotčeny.

V případě ukončení činnosti kvalifikovaného poskytovatele certifikačních služeb vyvine Česká pošta v souladu s § 13 [ZoEP] přiměřené úsilí pro převzetí správy zákazníků a související agendy jiným kvalifikovaným poskytovatelem certifikačních služeb. V tomto případě budou vztahy mezi tímto kvalifikovaným poskytovatelem a Českou poštou rovněž upraveny zvláštní smlouvou.

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

### 9.16.3 Oddělitelnost ustanovení

Žádná ustanovení v této kapitole.

### 9.16.4 Zřeknutí se práv

Žádná ustanovení v této kapitole.

### 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.

## 9.17Další opatření

### 9.17.1 Řídící dokumenty

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

| | |
|---|---|
| [CWA 141671] | CWA 14167-1:2003: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements |
| [ISO 17799] | ČSN ISO/IEC 17799: Informační technologie – Bezpečnostní techniky Soubor postupů pro management bezpečnosti informací |
| [ISO 27001] | ČSN ISO/IEC 27001:2006 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky |
| [RFC 2511] | Internet X.509 Certificate Request Message Format |
| [RFC 2560] | Internet X.509 Online Certificate Status Protocol (OCSP) |
| [RFC 3161] | Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) |
| [RFC 3280] | 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 |
| [RFC 5280] | Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile |
| [TR 13335] | ČSN ISO/IEC TR 13335: Informační technologie – Směrnice pro řízení bezpečnosti IT |
| [TS 101456] | ČSN ETSI TS 101 456 Elektronické podpisy a infrastruktury; Požadavky na postupy certifikační autority vydávající kvalifikované certifikáty, verze 1.3.1 |
| [TS 102023] | ČSN ETSI TS 102 023 Elektronické podpisy a infrastruktury; Požadavky na postupy autorit časových razítek |
| [V378] | Vyhláška Ministerstva informatiky č. 378/2006 Sb. ze dne 19. července 2006 o postupech kvalifikovaných poskytovatelů certifikačních služeb |
| [Z101] | Zákon č. 101/2000 Sb., o ochraně osobních údajů v platném znění |
| [Z300] | Zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů v platném znění |

[ZoEP] Zákon č. 227/2000 Sb. o elektronickém podpisu v platném znění

9.17.2 Odkazy a literatura

[VOP] Všeobecné obchodní podmínky certifikačních služeb