# Certifikační autorita PostSignum QCA České pošty, s.p.

## Certifikační politika PostSignum Qualified CA pro certifikáty určené pro ověření elektronického podpisu fyzické osoby

**Verze 1.16**

**30. června 2005**

**Česká pošta, s.p.**

Schváleno:

| Verze | Schválil | |
|---|---|---|
| 1.00 | Komise pro certifikační politiky | e-mail: paa.postsignum@cpost.cz |
| 1.15 | Komise pro certifikační politiky | e-mail: paa.postsignum@cpost.cz |
| 1.16 | Komise pro certifikační politiky | e-mail: paa.postsignum@cpost.cz |

# 1. ÚVOD

## 1.1 Upozornění pro uživatele certifikátu

Před použitím certifikátu vydaného podle této certifikační politiky pozorně pročtěte tento dokument a ujistěte se, že jste mu řádně porozuměli.

Zejména ověřte, že tato certifikační politika odpovídá vašemu certifikátu, neboť certifikační autorita PostSignum QCA vydává více typů certifikátů podle různých politik. Všechny tyto certifikační politiky můžete najít na WWW stránkách certifikační autority - www.postsignum.cz.

## 1.2 Přehled

Česká pošta, s.p. (dále i Česká pošta či ČP) ustavila dvouúrovňovou hierarchii certifikačních autorit s názvem PostSignum QCA. Kořenem této hierarchie je PostSignum Root QCA, která vydala certifikát pro certifikační autoritu PostSignum Qualified CA. PostSignum Qualified CA vydává kvalifikované certifikáty a kvalifikované systémové certifikáty koncových uživatelů, přičemž uplatňuje dva základní modely registrace v závislosti na "typu" koncového uživatele.

První model registrace je zaměřen na právnické osoby - organizace. Zákazník, který má zájem o služby PostSignum QCA uzavře s Českou poštou smlouvu o poskytování certifikačních služeb a definuje, které osoby smějí jménem zákazníka definovat, kterým zaměstnancům je dovoleno žádat o certifikáty podle jednotlivých certifikačních politik. Tento model umožňuje pre-registraci žadatelů o certifikát a zjednodušuje tak proces registrace žádosti na pracovišti registrační autority České pošty. Model rovněž umožňuje dohodnout se zákazníkem zvláštní podmínky procesu registrace, případně vznik nové certifikační politiky.

Druhý model registrace je zaměřen na jednotlivce - fyzické osoby. Vydání certifikátu fyzické osoby vyžaduje pouze jednu návštěvu pobočky České pošty, při které je s fyzickou osobou uzavřena smlouva o poskytování certifikačních služeb, a na základě přinesené digitální žádosti o certifikát je jí ihned vydán certifikát.

Tato certifikační politika upravuje vydávání kvalifikovaných certifikátů [ZoEP] určených pro ověření elektronického podpisu jednotlivce - fyzické osoby. Tyto osoby budeme nazývat fyzické podepisující osoby.

Fyzická osoba odpovídá za pravdivost údajů, které jsou v certifikátu uvedeny. PostSignum Qualified CA ověřuje vazbu mezi fyzickou osobou a veřejným klíčem v certifikátu.

Certifikáty vydané podle této politiky mohou být použity pouze pro ověření elektronického podpisu fyzické podepisující osoby v souladu se zákonem o elektronickém podpisu [ZoEP].

Fyzická osoba se osobně dostaví na libovolné pracoviště registrační autority České pošty, kde předloží dva své osobní doklady a médium s digitální žádostí o certifikát. Pokud jsou oba osobní doklady v pořádku a pokud na jejich základě byla ověřena totožnost fyzické osoby, uzavře s ní Česká pošta jednorázovou písemnou smlouvu o poskytování certifikačních služeb, kopie dokladů totožnosti ČP uchová v souladu se zákonem o elektronickém podpisu [ZoEP] ve znění pozdějších předpisů a zákonem č. 101/2000 Sb., ve znění pozdějších předpisů, o ochraně osobních údajů. Obsluha registrační autority ČP poté zkontroluje údaje v digitální žádosti o certifikát a případně požádá fyzickou osobu o předložení dalších dokladů, na základě kterých bude možné ověřit údaje ze žádosti. Pokud jsou všechny údaje v pořádku, je fyzické osobě vydán certifikát s veřejným klíčem z digitální žádosti. Fyzická osoba zkontroluje údaje uvedené v certifikátu a pokud s nimi souhlasí, písemně potvrdí převzetí certifikátu. Tímto okamžikem se fyzická osoba stává držitelem certifikátu - fyzickou podepisující osobou.

Plnění zásad této politiky rozpracovává a zajišťuje Certifikační prováděcí směrnice PostSignum QCA, verze 1.16, vydaná dne 30.6.2005.

Přílohy této certifikační politiky jsou uvedeny v kapitole 10. Přílohy.

### 1.2.1 Certifikační služby poskytované PostSignum Qualified CA

Certifikační autorita PostSignum Qualified CA nabízí tyto certifikační služby:

- vydání certifikátu podle existujících certifikačních politik,
- revokace certifikátu, vydání CRL a jeho zveřejnění,
- informace o stavu certifikátu,
- informace o vydaných certifikátech,
- informace o certifikátech QCA,
- informace o poskytovaných službách.

## 1.3 Identifikace politiky

Tab. 1 Identifikace politiky

| | |
|---|---|
| Název politiky | Politika pro certifikáty určené pro ověření elektronického podpisu fyzické osoby |
| Verze politiky | 1.16 |
| 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 | 2.23.134.1.4.1.5.116 |
| Datum vydání | 30.6.2005 |
| Doba platnosti | do odvolání |
| Odpovídající CPS | Certifikační prováděcí směrnice PostSignum QCA, verze 1.26 |

## 1.4 Zúčastněné strany a oblast použití

### 1.4.1 Poskytovatel certifikačních služeb

Poskytovatelem certifikačních služeb je Česká pošta, s.p.

### 1.4.2 PostSignum Root QCA

PostSignum Root QCA tvoří kořen hierarchie certifikačních autorit působících v rámci PostSignum QCA. Jejím úkolem je především vydávat a spravovat certifikáty certifikačních autorit působících v rámci České pošty.

### 1.4.3 PostSignum Qualified CA

Hlavním úkolem PostSignum Qualified CA v hierarchii PostSignum QCA je vydávat a spravovat certifikáty v souladu s definovanými certifikačními politikami.

### 1.4.4 Registrační autority

Fyzické osoby, které chtějí vydat nebo zneplatnit certifikát podle této politiky, přicházejí se svou žádostí na pracoviště registrační autority. Registrační autorita je pracoviště České pošty, jehož základním úkolem je přebírat žádosti o certifikát, kontrolovat identitu fyzických osob, poté přijmout nebo zamítnout žádost a předat vydaný certifikát držiteli. Na pracovišti registrační autority je možné podat žádost o zneplatnění certifikátu.

### 1.4.5 Klienti PostSignum Qualified CA

Klientem PostSignum Qualified CA je v případě certifikátu vydaného podle této certifikační politiky nepodnikající fyzická osoba.

## 1.5 Oblast použití

PostSignum Qualified CA vydává kvalifikované certifikáty určené k ověření elektronického podpisu a kvalifikované systémové certifikáty určené k ověření elektronické značky jak pro organizace, které požadují větší počet certifikátů, tak pro jednotlivce.

Kvalifikované certifikáty vydané podle této certifikační politiky mohou být použity pouze pro ověření elektronického podpisu fyzické osoby v souladu se zákonem o elektronickém podpisu [ZoEP].

### 1.5.1 Omezení použití certifikátu

Kvalifikované certifikáty vydávané podle této certifikační politiky je možné využívat pouze pro řádné a legální potřeby a v souladu s platnými právními předpisy.

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.

## 1.6 Správa certifikační politiky

### 1.6.1 Správce dokumentu

Za správu této certifikační politiky a za její soulad s dokumentem Certifikační a prováděcí směrnice odpovídá manažer QCA.

### 1.6.2 Komise pro certifikační politiky České pošty

Komise pro certifikační politiky České pošty (PAA ČP) je orgán, který ustavuje, sleduje a udržuje politiky, jimiž se řídí činnost PostSignum QCA. Jedná se jak o politiky pro kořenovou certifikační autoritu (PostSignum Root QCA), tak o politiky pro podřízené certifikační autority, tedy i PostSignum Qualified CA.

1.6.3 Správa dokumentu

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

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

- při vzniku nového typu certifikátu,
- při takové změně PostSignum QCA (např. změně postupů), která ovlivní obsah těchto dokumentů,
- pokud při pravidelné kontrole okolního prostředí PostSignum QCA byly identifikovány požadavky na změny těchto dokumentů.

1.6.4 Změny v certifikační politice

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

Veškeré změny v této certifikační politice podléhají schválení Komise pro certifikační politiky ČP (PAA ČP). PAA ČP přidělí nové verzi certifikační politiky číslo verze, které se promítne rovněž do identifikátoru politiky (OID).

Nová verze certifikační politiky bude zveřejněna na www serveru PostSignum QCA. PAA ČP rozhodne, zda je nutné zveřejnit informaci o nové verzi certifikační politiky též jinou formou, případně jak.

1.6.5 Platnost dokumentu

Platnost tohoto dokumentu je uvedena v kapitole 1.3.

1.6.6 Ukončení platnosti dokumentu

Platnost tohoto dokumentu je ukončena dnem ukončení platnosti posledního certifikátu vydaného podle této certifikační politiky.

1.7 Kontaktní informace

1.7.1 Poskytovatel certifikačních služeb

Poskytovatelem certifikačních služeb PostSignum Qualified CA je:

Česká pošta, s.p., IČ 47114983

se sídlem

Olšanská 38/9, 225 99 Praha 3

1.7.2 Provozní kontaktní údaje

S dotazy a požadavky spojenými s provozem PostSignum QCA, například s žádostmi o zneplatnění certifikátů, se obracejte na následující adresu:

Česká pošta, s.p.
OZ VAKUS
pracoviště autority PostSignum
Wolkerova 480
749 20 Vítkov

email: postsignum@cpost.cz
fax: +420 556 316 292
tel: +420 556 316 290

1.7.3 Správce dokumentu

Za správu tohoto dokumentu odpovídá manažer QCA. Kontaktní adresa manažera QCA je:

manager.postsignum@cpost.cz

1.7.4 Komise pro certifikační politiky České pošty

Komisi pro certifikační politiky ČP lze kontaktovat na adrese:

paa.postsignum@cpost.cz

1.7.5 PostSignum Root QCA

www server certifikační autority PostSignum Root QCA má adresu:

http://www.postsignum.cz

Adresářové služby certifikační autority PostSignum Root QCA jsou dostupné na adrese:

ldap://qca.postsignum.cz

Certifikát PostSignum Root QCA je zveřejněn rovněž v Poštovním věstníku.

1.7.6 PostSignum Qualified CA

Www server certifikační autority PostSignum Qualified CA má adresu:

http://www.postsignum.cz

Adresářové služby certifikační autority PostSignum Qualified CA jsou dostupné na adrese:

ldap://qca.postsignum.cz

1.7.7 Registrační autority (kontaktní pracoviště)

Aktuální seznam registračních autorit je k dispozici na www serveru PostSignum QCA.

1.7.8 Kontaktní osoba

Kontaktní osobou pro PostSignum Qualified CA je manažer QCA. Adresa kontaktní osoby:

manager.postsignum@cpost.cz

1.7.9 Osoba odpovědná za soulad CPS s CP

Osobou odpovědnou za soulad certifikační prováděcí směrnice s touto politikou je manažer QCA, jehož adresa je:

manager.postsignum@cpost.cz

1.8 Použité zkratky a pojmy

**QCA ČP** - viz. PostSignum QCA

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

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

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

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

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

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

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

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

**Obchodní místo** – centrální regionální pracoviště odpovědné za uzavírání a evidenci smluv (typicky se jedná o pracoviště marketingu PTJ VT).

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

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

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

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

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

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

**Žadatel** - osoba, která má právo žádat u PostSignum Qualified CA o certifikát podle některé z platných certifikačních politik.

## 2. ZVEŘEJŇOVÁNÍ A UCHOVÁVÁNÍ INFORMACÍ

### 2.1 Uložení dat, jejich správa a zásady zveřejňování

Vydané certifikáty jsou uloženy v adresářovém serveru České pošty, s.p. a v databázi certifikační autority.

Informace o vydaných certifikátech a jejich stavu (prostřednictvím seznamu zneplatněných certifikátů - CRL) a seznamech zneplatněných certifikátů jsou poskytovány prostřednictvím adresářových služeb a pomocí www rozhraní na www serveru PostSignum QCA.

Prostřednictvím adresářového serveru i www rozhraní jsou přístupné pouze ty certifikáty (a s nimi spojené informace), u nichž zákazník (držitel certifikátu) souhlasil se zveřejněním.

Poskytovány jsou tyto služby:

- vyhledání certifikátu s daným sériovým číslem,
- vyhledání certifikátů podle zadané e-mailové adresy,
- vyhledání certifikátů pro zadaný objekt,
- výpis certifikátů certifikační autority,
- zpřístupnění CRL,
- stažení certifikátu.

Přístup k těmto službám není nijak omezen.

### 2.2 Zveřejňování certifikátů a CRL

Certifikáty a CRL jsou přístupné na adresách

http://www.postsignum.cz

ldap://qca.postsignum.cz

ldap://postsignum.ttc.cz

CRL je zveřejňován rovněž na adrese

http://postsignum.ttc.cz/crl/psqualifiedCA.crl

2.3 Zveřejňování informací o certifikační autoritě

Každá certifikační autorita v hierarchii PostSignum QCA zveřejňuje své certifikační politiky na www serveru PostSignum QCA.

Zde jsou zveřejněny také certifikáty certifikačních autorit včetně PostSignum Root QCA, jejíž certifikát a otisk tohoto certifikátu jsou navíc zveřejněny v Poštovním věstníku.

2.4 Periodicita zveřejňování

Certifikáty vydané PostSignum Qualified CA, u nichž byl vysloven souhlas se zveřejněním, jsou zveřejňovány elektronickou cestou nejpozději do 24 hodin od převzetí certifikátu držitelem (viz odstavec 4.4).

Seznamy zneplatněných certifikátů (CRL) jsou zveřejňovány alespoň jednou za dvanáct hodin. V případě zneplatnění certifikátu vydaného PostSignum Qualified CA je CRL, na němž je tento certifikát uveden, zveřejněn do dvanácti hodin od přijetí žádosti o zneplatnění certifikátu.

Nové certifikační politiky a revize stávajících politik jsou zveřejňovány na www serveru PostSignum QCA po schválení Komisí pro certifikační politiky ČP a jejich vydání.

2.5 Řízení přístupu k informacím

Certifikační politiky, certifikáty certifikačních autorit a seznamy zneplatněných certifikátů jsou přístupné pro čtení bez jakéhokoliv omezení.

Poskytovatel certifikačních služeb neumožňuje přístup k vydaným certifikátům, u kterých nebyl držitelem vysloven souhlas se zveřejněním. Přístup k vydaným certifikátům, u kterých byl držitelem vysloven souhlas se zveřejněním, je omezen na vyhledání těchto certifikátů podle zadaného kriteria.

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

## 3. IDENTIFIKACE A AUTENTIZACE

3.1 Uzavření smlouvy s fyzickou osobou

Fyzická osoba uzavírající smlouvu o poskytování certifikačních služeb prokazuje svou totožnost dvěma osobními doklady, z nichž jeden musí být platný občanský průkaz pro občany České republiky a pro občany jiných států platný cestovní pas. Další akceptované doklady jsou platný cestovní pas, řidičský průkaz, průkaz ZTP, rodný list a pro cizince povolení k pobytu a řidičský průkaz Evropské unie.

Pracovník registrační autority zkontroluje:

- zda jsou doklady platné,

- zda fotografie na dokladu odpovídá žadateli o certifikát.

Smlouva je uzavřena pouze tehdy, pokud jsou splněny všechny výše uvedené podmínky.

Smlouva o poskytování certifikačních služeb uzavíraná mezi Českou poštou a fyzickou osobou je písemná a vztahuje se pouze na jednorázové vydání certifikátu.

3.2 Registrace žádosti o certifikát

Identita žadatele o certifikát je ověřena během procesu uzavření smlouvy, který bezprostředně předchází zpracování žádosti.

3.3 Registrace žádostí o zneplatnění certifikátů

Držitel certifikátu, který žádá o zneplatnění certifikátu, prokáže svou totožnost:

- znalostí hesla pro zneplatnění, které zadal při registraci žádosti o certifikát, nebo

- dvěma osobními doklady obdobně jako při registraci žádosti o certifikát.

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

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

3.4 Registrace žádostí o obnovu certifikátu

Obnova certifikátu probíhá stejně jako registrace první žádosti a vydání prvního certifikátu podepisující osobě.

3.5 Znakové sady a transkripce údajů

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

- UTF8, znaky středoevropské znakové sady,

- US ASCII.

Veškeré údaje dokladované fyzickou 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 a průkazech totožnosti. Transkripce, jako například odstranění diakritiky, není možná.

E-mailová adresa uvedená v rozšíření SubjectAltName certifikátu může být kódována pouze znakovou sadou US ASCII.

3.6 Jednoznačnost jmen

Česká pošta přiřazuje každé fyzické osobě, která žádá o certifikát podle této certifikační politiky, jednoznačný identifikátor zákazníka ČP v rámci autority vydávající certifikáty podle této politiky. V položce Subject certifikátu je uvedena kombinace údajů o držiteli (jméno a příjmení, vari-

antně adresa) a jednoznačný identifikátor přidělený Českou poštou. Tím je zaručeno, že dvěma různým fyzickým osobám nebudou vydány certifikáty se stejnou položkou Subject.

3.7 Pseudonym

PostSignum Qualified CA nepodporuje pseudonym fyzické osoby v položce Subjekt certifikátu.

3.8 E-mailová adresa

E-mailová adresa držitele certifikátu je umístěna v nepovinném rozšíření certifikátu Subject Alternative Name. Česká pošta, jakožto poskytovatel certifikačních služeb, neověřuje existenci e-mailové adresy ani její vztah k držiteli certifikátu. Tuto položku proto nelze použít pro identifikaci držitele certifikátu.

3.9 Postup v případě kolize jmen

V případě kolize rozlišovacích jmen dvou fyzických osob, a tím i kolize položky Subject v certifikátech těchto dvou osob, rozhodne o řešení manažer QCA a toto řešení navrhne postiženým fyzickým osobám do dvou pracovních dní od vzniku kolize.

## 4. PROVOZNÍ POŽADAVKY

4.1 Uzavření smlouvy

Fyzická osoba se dostaví na libovolné pracoviště registrační autority České pošty, kde je s ní projednána nabídka certifikačních služeb a vyplněna smlouva o poskytování certifikačních služeb (dále smlouva). Smlouva obsahuje mimo jiné:

- identifikační údaje fyzické osoby včetně celého jména a adresy trvalého bydliště,
- typy požadovaných certifikačních služeb a jejich cenu,
- platební podmínky.

Smlouva je fyzickou osobou podepsána na pracovišti registrační autority ČP. Smlouva musí být v písemné formě.

Cena za vydané certifikáty je buď zahrnuta v ceně jiné služby nebo je fyzickou osobou uhrazena na pobočce České pošty, s.p. nejpozději při převzetí vydaného certifikátu.

Česká pošta si vyhrazuje právo neuzavřít s fyzickou osobou smlouvu o poskytování certifikačních služeb.

4.2 Registrace žádosti o certifikát a vydání certifikátu

Fyzická osoba dokládá při registraci žádosti o certifikát tyto údaje

Tab.2 Registrace žádosti

| **Dokladovaný údaj** | **Doklad** | **Poznámka** |
|---|---|---|
| Jméno a příjmení | Občanský průkaz, pas, řidičský průkaz, průkaz ZTP | |
| Titul | Občanský průkaz, pas, řidičský průkaz, vysokoškolský diplom | Pokud má být v certifikátu uvedeno. |
| Adresa trvalého bydliště | Libovolný z akceptovaných dokladů. | Pokud má být v certifikátu uvedeno. |

U osob s trvalým bydlištěm na území státu EU může být součástí adresy trvalého bydliště označení příslušného státu. Pro označení státu se používají dvoumístné aplha2 kódy podle ISO3166. Převod mezi označením státu uvedeným na předloženém dokladu a použitým kódem provádí pracovník registrační autority.

V certifikátu fyzických osob může být jako volitelná položka uvedena adresa elektronické pošty žadatele. Pokud ji bude fyzická osoba chtít mít v certifikátu uvedenu, odpovídá za její správnost.

Některé z uvedených údajů jsou mapovány do položek uvedených v certifikátu, jak je uvedeno v Tab. 3.

Tab.3 Mapování údajů

| **Požadovaný údaj** | **Údaj v certifikátu** |
|---|---|
| Jméno a příjmení, titul | Položka Subject, atribut CN |
| Adresa trvalého bydliště | Položka Subject, nepovinný atribut L |
| Adresa elektronické pošty | Rozšíření SubjectAltName - rfc822 email |

Fyzická osoba předloží na pracovišti registrační autority své dva osobní doklady a digitální žádost ve formátu PKCS#10 obsahující veřejný klíč, která je podepsána soukromým klíčem odpovídajícím veřejnému klíči uvedenému v žádosti. Tím je prokázáno, že fyzická osoba v době vytváření žádosti vlastnila soukromý klíč odpovídající veřejnému klíči uvedenému v žádosti. Fyzická osoba dále sdělí, zda si přeje uvést v certifikátu, o který žádá, identifikátor klienta MPSV.

Pracovník registrační autority zkontroluje osobní doklady fyzické osoby, vytvoří a uloží jejich kopie. Na základě digitální žádosti o certifikát pak zavede fyzickou osobu do systému pro správu žadatelů České pošty. Před zavedením údajů do tohoto systému pracovník registrační autority zkontroluje, zda je fyzická osoba schopna údaje ze žádosti o certifikát řádně doložit. Pokud se údaje ze žádosti liší od údajů v osobních nebo úředních dokladech, upraví pracovník registrační autority údaje v žádosti tak, aby se s příslušnými doklady shodovaly. Pokud fyzická osoba s úpravou nesouhlasí, nemůže jí být certifikát vydán.

Fyzická osoba při registraci zadává rovněž heslo, pomocí kterého bude certifikát v případě potřeby zneplatňovat, a vyjadřuje svůj souhlas nebo nesouhlas se zveřejněním vydaného certifikátu prostřednictvím služeb poskytovatele.

Jakmile jsou všechny údaje v pořádku, pracovník registrační autority vytiskne papírový protokol žádosti o certifikát a předloží jej k podpisu fyzické osobě. Tento protokol se stane přílohou smlouvy o poskytování certifikačních služeb. Poté, co fyzická osoba protokol podepíše, schválí pracovník registrační autority vydání certifikátu.

Pokud má pracovník registrační autority pochybnosti o předložených dokladech nebo pokud se vyskytnou jiné nesrovnalosti, odmítne certifikát vydat.

Česká pošta si rovněž vyhrazuje právo odmítnout vydání certifikátu fyzické osoby podle této certifikační politiky.

## 4.3 Vydání certifikátu

Poskytovatel certifikačních služeb je povinen do dvou pracovních dnů od podání žádosti posoudit žádost o certifikát, vydat rozhodnutí, zda bude certifikát vydán, a o tomto rozhodnutí informovat žadatele o certifikát. Od okamžiku rozhodnutí je poskytovatel povinen vydat certifikát do následujícího pracovního dne.

Po zpracování žádosti o certifikát vloží operátor registrační autority 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 registrační autoritě a publikačním službám.

Certifikát se stává platným okamžikem vydání.

## 4.4 Převzetí certifikátu

Poté, co je certifikát vydán, žadatel o certifikát zkontroluje správnost údajů uvedených v certifikátu a podepíše protokol o převzetí certifikátu, ve kterém je obsaženo rovněž upozornění na povinnosti, které z používání certifikátu vyplývají.

Podpisem protokolu o převzetí certifikátu žadatel stvrzuje:

- že na sebe bere závazky vyplývající z certifikační politiky, podle které byl certifikát vydán,
- že mu nejsou známy žádné skutečnosti, které by svědčily o tom, že soukromý klíč odpovídající veřejnému klíči v certifikátu vlastní jiná osoba, než je povoleno v příslušné certifikační politice,
- že údaje, které byly přeneseny ze žádosti o certifikát do certifikátu, jsou správné a úplné.

Žadatel o certifikát dále zaplatí cenu za vydání certifikátu. Po převzetí certifikátu se žadatel o certifikát stává držitelem certifikátu a také podepisující osobou.

Vydaný certifikát je podepisující osobě předán na disketě ve formátu DER spolu s certifikátem vydávající certifikační autority PostSignum Qualified CA a s certifikátem kořenové certifikační autority PostSignum Root QCA. Certifikáty autorit jsou rovněž ve formátu DER.

Obsluha registrační autority předá podepisující osobě vydaný certifikát rovněž ve formátu PEM nebo PKCS#7, pokud o to podepisující osoba požádá.

## 4.5 Obnova certifikátu

Obnova certifikátu vydaného podle této certifikační politiky není možná. Po ukončení platnosti stávajícího certifikátu požádá podepisující osoba o vydání nového certifikátu, není nutné měnit subjekt certifikátu podepisující osoby.

## 4.6 Použití klíče a certifikátu

Páry klíčů svázané s certifikáty mají stejnou dobu platnosti jako certifikáty. Klíčové páry, jejichž platnost vypršela, nemohou být v prostředí PostSignum Qualified CA znovu použity.

## 4.7 Zneplatnění certifikátu

### 4.7.1 Důvody zneplatnění certifikátu

Důvody pro zneplatnění certifikátu koncového uživatele jsou především následující:

- jakékoliv podezření na kompromitaci odpovídajícího soukromého klíče,
- neplnění podmínek smlouvy o poskytování certifikačních služeb ze strany zákazníka,
- příkaz orgánu definovaného zákonem o elektronickém podpisu,
- příslušná žádost držitele, podepisující nebo označující osoby a
- další důvody uvedené v [ZoEP] (úmrtí, zánik, zbavení nebo omezení právní způsobilosti podepisující resp. označující osoby; pozbytí pravdivosti údajů, na jejichž základě byl certifikát vydán).

### 4.7.2 Osoby oprávněné žádat o zneplatnění certifikátu

O zneplatnění certifikátu může požádat držitel certifikátu, manažer certifikační autority, která vydala certifikát, nebo zástupce orgánu definovaného zákonem o elektronickém podpisu.

### 4.7.3 Postup zneplatnění na žádost držitele certifikátu

#### 4.7.3.1 Žádost o zneplatnění certifikátu podaná osobně podepisující osobou na registrační autoritě

Podepisující osoba požádá o zneplatnění certifikátu osobně na přepážce registrační autority, kde prokáže svou totožnost obdobně jako při podávání žádosti o certifikát. Vyplní písemnou žádost o zneplatnění certifikátu, obsahující sériové číslo certifikátu a volitelně i důvod zneplatnění.

Operátor registrační autority vyhledá certifikát a zahájí proces zneplatnění. Vyhledá podepisující osobu v evidenci žadatelů a ověří její právo žádat o zneplatnění certifikátu. Pokud ověření proběhne úspěšně, odešle operátor registrační autority žádost o zneplatnění do systému certifikační autority ke zpracování. Po zpracování žádosti systémem certifikační autority ověří operátor stav certifikátu a vytiskne a předá podepisující osobě protokol o zneplatnění certifikátu. Podepisující osoba protokol podepíše.

#### 4.7.3.2 Žádost o zneplatnění certifikátu podaná písemně, faxem, telefonicky nebo jiným vzdáleným způsobem

Podepisující osoba podává žádost o zneplatnění certifikátu telefonicky, písemně nebo faxem na telefonní číslo nebo adresu uvedenou v certifikační politice nebo jiným vzdáleným způsobem specifikovaným na www serveru poskytovatele. Služba pro telefonické zneplatnění je dostupná 24 hodin denně. Každá takto podaná žádost obsahuje sériové číslo certifikátu, heslo pro zneplatnění certifikátu a volitelně důvod zneplatnění. Písemná žádost je podepsána podepisující osobou.

Operátor oprávněný provádět zneplatnění zkontroluje heslo pro zneplatnění v žádosti oproti heslu uvedenému v protokolu o převzetí certifikátu. V případě, že údaje souhlasí, certifikát je zneplatněn. V případě, že certifikát nelze zneplatnit na základě údajů v žádosti uvedených, operátor zneplatnění neprovede a informuje podepisující osobu.

Pokud bylo zneplatnění úspěšné, je vytvořen protokol o zneplatnění, který je zaslán podepisující osobě.

4.7.4 Zneplatnění certifikátu z vůle certifikační autority

O revokaci certifikátu může rozhodnout rovněž poskytovatel certifikačních služeb, například pokud podepisující osoba porušuje pravidla certifikační politiky nebo dohodnuté smluvní podmínky. PostSignum QCA v takovém případě informuje zákazníka o zneplatnění certifikátu s udáním důvodu, proč byl certifikát revokován. Manažer QCA podává písemnou žádost o zneplatnění certifikátu, kterou předá některému z operátorů oprávněných provádět zneplatnění certifikátu.

Po úspěšném zneplatnění je vytvořen protokol o zneplatnění certifikátu, který je neprodleně zaslán zákazníkovi. Zákazník je o zneplatnění certifikátu z vůle poskytovatele informován rovněž prostřednictvím elektronické pošty, pokud vlastní certifikát vydaný PostSignum Qualified CA, ve kterém je uvedena jeho e-mailová adresa.

4.7.5 Zneplatnění certifikátu z vůle orgánu definovaného zákonem o elektronickém podpisu.

O revokaci certifikátu vydaného jako kvalifikovaný může rozhodnout, jakožto o předběžném opatření, rovněž orgán definovaný zákonem o elektronickém podpisu. PostSignum QCA v takovém případě informuje zákazníka o zneplatnění certifikátu s udáním důvodu, proč byl certifikát revokován. Zástupce orgánu definovaného zákonem o elektronickém podpisu podává písemnou žádost o zneplatnění certifikátu manažerovi QCA.

Po úspěšném zneplatnění je vytvořen protokol o zneplatnění certifikátu, který je neprodleně zaslán zákazníkovi společně s důvodem zneplatnění certifikátu. Zákazník je o zneplatnění certifikátu z vůle orgánu definovaného zákonem o elektronickém podpisu informován rovněž prostřednictvím elektronické pošty, pokud vlastní certifikát vydaný PostSignum Qualified CA, ve kterém je uvedena jeho e-mailová adresa.

4.7.6 Časová prodleva od podání žádosti o zneplatnění

Doba od podání žádosti o zneplatnění certifikátu do zveřejnění CRL obsahujícího i zneplatněný certifikát nepřesáhne 12 hodin.

4.8 Identifikátor klienta MPSV

Certifikační autorita PostSignum QCA České pošty umožňuje umístit do kvalifikovaného certifikátu vydaného podle této certifikační politiky identifikátor klienta, přidělovaný občanům ČR Ministerstvem práce a sociálních věcí (dále IK MPSV). IK MPSV je umístěn do nepovinného rozšíření certifikátu Subject Alternative Name - Other Name.

Česká pošta na základě údajů získaných od zákazníka zprostředkuje přidělení identifikátoru klienta od Ministerstva práce a sociálních věcí a to bezplatně.

Česká pošta bude zprostředkovávat přidělení identifikátoru klienta pouze za účelem uvedení tohoto identifikátoru ve vydávaných kvalifikovaných certifikátech.

4.9 Informace o stavu certifikátu

Seznam zneplatněných certifikátů (CRL) je zveřejňován alespoň každých 12 hodin na třech místech:

- na www serveru PostSignum QCA,
- v adresářových službách PostSignum QCA,

- u nezávislého poskytovatele www a adresářových služeb.

Primárním zdrojem aktuálního CRL je www server PostSignum QCA.

PostSignum Qualified CA neposkytuje informace o stavu certifikátu protokolem OCSP.

4.10 Konec platnosti certifikátu

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

Pokud není certifikát po dobu jeho platnosti nutné zneplatnit, skončí jeho platnost v časovém okamžiku uvedeném v certifikátu. Každý vydaný certifikát zůstává po ukončení své platnosti nadále uložen v databázi vydávající certifikační autority a archivován v souladu s platnou legislativou a archivačními předpisy České pošty. Pokud byl držitelem vysloven souhlas se zveřejněním certifikátu, je takový certifikát nadále přístupný na www a adresářovém serveru PostSignum QCA.

## 5. BEZPEČNOST FYZICKÁ, PROCEDURÁLNÍ A PERSONÁLNÍ

Fyzická, procedurální a personální bezpečnost PostSignum QCA se řídí platnými předpisy České pošty. Tato kapitola je podrobně rozpracována v Certifikační prováděcí směrnici.

5.1 Ukončení činnosti PostSignum Qualified CA

Ukončení činnosti PostSignum Qualified CA musí být písemně oznámeno všem držitelům platných certifikátů a rovněž zveřejněno na www serveru PostSignum uvedeném v kapitole 1.7.6 a na všech kontaktních místech 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 PostSignum Qualified CA 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 PostSignum Qualified CA ukončena.

Zneplatněný kvalifikovaný systémový certifikát PostSignum Qualified CA bude zveřejněn na CRL PostSignum Root QCA nejpozději 12 hodin po jeho zneplatnění.

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

ČP prokazatelně zničí data pro vytváření elektronického podpisu PostSignum Qualified CA, která sloužila pro podepisování kvalifikovaných certifikátů a seznamů zneplatněných certifikátů.

5.1.1 Podezření na kompromitaci soukromého klíče PostSignum Qualified CA

V případě podezření na kompromitaci soukromého klíče PostSignum Qualified CA budou písemně informováni všichni držitelé certifikátů o mimořádném ukončení činnosti této autority, oznámení bude rovněž zveřejněno na www serveru PostSignum uvedeném v kapitole 1.7.6 a na všech pracovištích registrační autority PostSignum QCA. Součástí oznámení bude i důvod ukončení platnosti certifikátu podřízené certifikační autority.

PostSignum Root QCA okamžitě zneplatní certifikát PostSignum Qualified CA, zneplatněný certifikát bude nejpozději do 12 hodin zveřejněn na CRL PostSignum Root QCA.

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

Česká pošta prokazatelně zničí data pro vytváření elektronického podpisu PostSignum Qualified CA, která sloužila pro podepisování kvalifikovaných certifikátů a seznamů zneplatněných certifikátů, u nichž existuje podezření na kompromitaci.

5.2 Ukončení činnosti kvalifikovaného poskytovatele certifikačních služeb

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

## 6. TECHNICKÁ BEZPEČNOST

Česká pošta, jakožto poskytovatel certifikačních služeb, věnuje náležitou péči ochraně párových dat certifikačních autorit a komponent PKI v hierarchii PostSignum QCA. Tato kapitola je podrobně rozpracována v Certifikační prováděcí směrnici.

6.1 Ochrana klíčů autority

Soukromý klíč PostSignum Qualified CA je generován a uschováván v zařízení, které splňuje požadavky standardu FIPS 140-1 Level 4. Použité algoritmy a jejich parametry odpovídají požadavkům zákona o elektronickém podpisu [ZoEP] v platném znění a navazujících předpisů. Délka klíče pro algoritmus RSA je 2048 bitů.

6.2 Ochrana klíčů držitelů certifikátů

Soukromé klíče držitelů certifikátů jsou generovány a uschovávány držitelem certifikátů. Jedná se o klíče pro algoritmus RSA, s délkou 1024 nebo 2048 bitů. PostSignum Qualified CA s těmito klíči nepřichází do styku, není zodpovědná za jejich ochranu ani zálohování.

Obecně je však možné držitelům certifikátů doporučit následující pravidla jako absolutní bezpečnostní minimum:

- ukládat soukromé klíče do speciálních, k tomu určených zařízení (např. čipových karet) nebo alespoň do zašifrovaného souboru,
- heslo pro zpřístupnění zařízení nebo zašifrovaného souboru obsahujícího soukromý klíč držet pod svou výhradní kontrolou (nesdělovat jiné osobě),
- jako heslo volit těžko uhádnutelný řetězec o dostatečné délce (min. 8 znaků),
- používat soukromý klíč na důvěryhodných systémech.

# 7. PROFIL CERTIFIKÁTU, CRL A ŽÁDOSTI O CERTIFIKÁT

Tab. 4 Profil certifikátu fyzické podepisující osoby

| | |
|---|---|
| Version | 3 (0x2) |
| Serial Number | *PostSignum Qualified CA přiřazuje každému vydanému certifikátu jednoznačné číslo.* |
| SignatureAlgorithm | sha1WithRSAEncryption |
| Issuer | |
| Country | CZ |
| Organisation | Česká pošta, s.p. [IČ 47114983]<br>*uvedené číslo je IČ České pošty, s.p.* |
| CN | PostSignum Qualified CA |
| Validity | |
| Not Before | *Datum vydání - UTCTime* |
| Not After | *1 rok od data vydání - UTCTime* |
| Subject | |
| Country | CZ |
| Locality | *Město nebo*<br>*Město ulice číslo nebo*<br>*Dvoumístný alpha2 kód státu EU podle ISO3166 město nebo*<br>*Dvoumístný alpha2 kód státu EU podle ISO3166 město ulice číslo*<br><br>*Trvalé bydliště žadatele*<br>*Nepovinná položka* |
| OU | *Jednoznačný identifikátor přidělený Českou poštou* |
| CN | *Jméno a příjmení (v uvedeném pořadí), případně i titul(y) fyzické podepisující osoby podle předložených dokladů* |
| Subject Public Key Info | |
| Algorithm | rsaEncryption |
| SubjectPublicKey | *veřejný klíč podepisující osoby* |
| Extensions | *rozšíření certifikátu podle tabulky 5* |
| Signature | *elektronická značka poskytovatele certifikačních služeb* |

Položka Subject certifikátu jednoznačně identifikuje fyzickou podepisující osobu.

Tab. 5 Rozšíření v certifikátu

| Název rozšiřující položky | Hodnota/příznak použití | Kritická ano/ne |
|---|---|---|
| Authority Key Identifier | | ne |
| Key Identifier | *používá se* | |
| AuthorityCertIssuer | *používá se* | |
| AuthorityCertSerialNumber | *používá se* | |
| Subject Key Identifier | *používá se* | ne |
| Subject Alternative Name | | |
| RFC822 Email address | *adresa elektronické pošty - údaj ze žádosti* | ne |
| OtherName | *IK MPSV* | ne |
| Key Usage | | ano |
| digitalSignature | ano | |
| nonRepudiation | ano | |
| keyEncipherment | ano | |
| dataEncipherment | ne | |
| keyAgreement | ne | |
| keyCertSign | ne | |
| cRLSign | ne | |
| CertificatePolicies | | ne |
| Policy Identifier | 2.23.134.1.4.1.5.116 | |
| Policy Qualifier id | CPS | |
| CPS URI | http://www.postsignum.cz | |
| User Notice | Tento certifikat byl vydan jako kvalifikovany certifikat ve smyslu zakona 227/2000 Sb. a navazujicich predpisu. | |
| Qualified certificate statement | | ne |
| OID | 0.4.0.1862.1.1<br>*(esi4-QCStatement-1: Compliance with Annex I and II of EU Directive 1999/93/EC)* | |
| | | |
| CRL Distribution Points | URI:<br>http://www.postsignum.cz/crl/psqualifiedca.crl<br>URI:<br>http://postsignum.ttc.cz/crl/psqualifiedca.crl<br>URI:<br>ldap://qca.postsignum.cz/ cn=PostSignum Qualified CA,o=Ceska posta s.p. [IC 47114983], c=CZ<br>URI:<br>ldap://postsignum.ttc.cz/ cn=PostSignum Qualified CA,o=Ceska posta s.p. [IC 47114983],c=CZ | ne |
| Basic Constraints | cA:FALSE | ne |

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

Tab. 6 Profil CRL

| | |
|---|---|
| Version | 2 (0x1) |
| Issuer Distinguished Name | |
| Country | CZ |
| Organisation | Česká pošta, s.p. [IČ 47114983] |
| CN | PostSignum Qualified CA |
| Validity | |
| This Update | *Datum vydání* |
| Next Update | *Datum vydání + 12 hodin* |
| RevokedCertificates | *opakující se položka pro každý zneplatněný certifikát* |
| UserCertificate | *sériové číslo zneplatněného certifikátu* |
| RevocationDate | *datum a čas zneplatnění* |
| CrlEntryExtensions | *rozšíření položky CRL podle tabulky 7* |
| CrlExtensions | *rozšíření CRL podle tabulky 7* |
| SignatureAlgorithm | sha1WithRSAEncryption |
| Signature | *elektronická značka poskytovatele certifikačních služeb* |

Tab. 7 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 | *PostSignum Qualified CA přiřadí každému CRL jednoznačné číslo.* | ne |

## 7.1 Žádost o certifikát

Česká pošta přijímá elektronické žádosti o certifikát ve formátu PKCS#10, kódování DER a BASE64. Součástí elektronické žádosti o certifikát musí být veřejný klíč žadatele o certifikát a dále tyto položky:

Tab. 8 Profil žádosti o certifikát

| Položka | Obsah | Poznámka |
|---|---|---|
| Subject | | |
| Country | CZ | |
| Locality | *Město nebo*<br>*Město ulice číslo nebo*<br>*Dvoumístný alpha2 kód státu EU podle ISO3166 město nebo*<br>*Dvoumístný alpha2 kód státu EU podle ISO3166 město ulice číslo*<br><br>*Trvalé bydliště fyzické osoby*<br>*Nepovinná položka* | Pokud má být v certifikátu uvedeno. |
| CN | *Jméno a příjmení (v uvedeném pořadí), případně i titul(y) fyzické podepisující osoby podle předložených dokladů* | |
| Extensions | | |
| SubjectAltName | *E-mailová adresa* | Pokud má být v certifikátu uvedeno. Rozšíření certifikátu. |

## 8. HODNOCENÍ SHODY A SOULADU S PŘEDPISY

8.1 Audit

Činnost PostSignum QCA podléhá auditu. Audit PostSignum QCA provádí nejméně jednou čtvrtletně interní auditor, jednou ročně je provoz PostSignum Qualified CA prověřen externím auditorem nezávislým na České poště, s.p.

8.2 Oblasti auditu

V rámci pravidelného interního auditu je hodnocen běžný provoz PostSignum QCA. Interní audity provádí Auditor QCA.

Oblasti hodnocené v rámci pravidelných externích auditů jsou specifikovány v certifikační prováděcí směrnici.

8.3 Opatření v případě zjištění nedostatků

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

8.4 Archivace záznamů

Záznamy o činnosti PostSignum QCA jsou archivovány po dobu deseti let.

8.4.1 Typy uchovávaných archivních záznamů

V PostSignum QCA se archivují tyto záznamy:

- programové vybavení a data, včetně vydaných certifikátů a CRL,
- veškerá papírová 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.

## 9. DALŠÍ OBCHODNÍ A PRÁVNÍ ZÁSADY

### 9.1 Poplatky za služby

Cena za poskytnuté certifikační služby je stanovena ve smlouvě mezi fyzickou osobou a poskytovatelem certifikačních služeb a řídí se aktuálním platným ceníkem. Cena za vydané certifikáty je buď zahrnuta v ceně jiné služby nebo je fyzickou osobou uhrazena na pobočce České pošty, s.p.

### 9.2 Finanční odpovědnost

#### 9.2.1 Pojistné krytí

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

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

#### 9.2.2 Aktiva ČP

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

K nahlédnutí je též na www serveru České pošty (www.cpost.cz).

### 9.3 Ochrana důvěrných informací

V maximálním rozsahu podle mandatorních 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. Bez ohledu na výše uvedená ustanovení se za důvěrné přitom nepovažují informace, které:

- se staly veřejně známými, aniž by to zavinila záměrně či opominutím 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, a nebo je nezíská nezákonným způsobem, o čemž by přijímající strana věděla nebo vědět musela,
- jsou uvedené na kvalifikovaném certifikátu, pokud k jeho zveřejnění dal držitel souhlas.

Závazek dle předchozího ustanovení zůstává v platnosti i po ukončení platnosti smlouvy o poskytování certifikačních služeb, a to po celou dobu, kdy je jeho porušení schopné způsobit škodu.

## 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, všeobecných obchodních podmínkách ČP [VOP] a v certifikační a prováděcí směrnici [CPS] a vycházejí z příslušných ustanovení zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.

Česká pošta poskytuje informace v rozsahu upraveném touto certifikační politikou držitelům, podepisujícím osobám nebo spoléhajícím se osobám, jakož i auditorům pro účely vyjádření shody - auditu dle odst. 2.7 výše, a dále poskytování informací v nezbytném rozsahu na základě mandatorních ustanovení platných právních předpisů (např. orgánům činným v trestním řízení v případech požadovaných v trestněprávních předpisech).

### 9.4.1 Souhlas se zpracováním osobních údajů

Žadatel o certifikát dává během procesu registrace žádosti o certifikát České poště souhlas se zpracováním osobních údajů nutných pro zavedení žadatele do systému PostSignum QCA.

Žadatel dále dává České poště souhlas se zpracováním svého rodného čísla.

V případě, že si žadatel o certifikát přeje mít v certifikátu vydaném PostSignum QCA uveden Identifikátor klienta MPSV, dává během procesu registrace žádosti o certifikát České poště souhlas s poskytnutím osobních údajů Ministerstvu práce a sociálních věcí za účelem přidělení identifikátoru klienta a dále souhlas s uvedením IK MPSV v certifikátu.

### 9.4.2 Zpřístupnění osobních údajů orgánům zmocněným ze zákona

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

### 9.4.3 Zpřístupnění informací na základě požadavku klienta

PostSignum QCA poskytuje klientovi v souladu se zákonem [Z101] informace o osobních údajích, které PostSignum QCA o dané osobě udržuje.

## 9.5 Ochrana 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 webové stránky certifikační autority (www.postsignum.cz).

## 9.6 Záruky ČP

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

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

## 9.7 Omezení záruk

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

Česká pošta neodpovídá za vady poskytnutých služeb vzniklé z důvodu nesprávného nebo neoprávněného využívání služeb 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.

## 9.8 Odpovědnost

### 9.8.1 Odpovědnost ČP

a) Omezení odpovědnosti za škodu - pokud nevyplývá z mandatorních ustanovení platných právních předpisů jinak, odpovídá Česká pošta držiteli certifikátu za škodu způsobenou porušením povinností České pošty v souvislosti s plněním smlouvy o poskytování certifikačních služeb.

b) Česká pošta neodpovídá za škodu vyplývající z použití kvalifikovaného certifikátu, pokud došlo ze strany držitele a nebo spoléhající se osoby k nedodržení omezení pro jeho použití, uvedených v této certifikační politice a zveřejněném na webové stránce PostSignum QCA.

c) Česká pošta neodpovídá za škodu vyplývající z použití kvalifikovaného certifikátu v období po podání žádosti o jeho zneplatnění, pokud Česká pošta dodrží lhůtu pro zveřejnění zneplatněného kvalifikovaného certifikátu na seznamu zneplatněných certifikátů (CRL), uvedenou v kapitole 2 této certifikační politiky.

d) 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.

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

#### 9.8.1.1 Odpovědnost registračních autorit

Odpovědnost registračních autorit je stanovena certifikační politikou a obecně závaznými právními předpisy. Vzhledem k tomu, že pracovníci registračních autorit jsou zaměstnanci ČP, pro jejich odpovědnost platí omezení podle interních předpisů České pošty.

9.8.2 Odpovědnost držitele, podepisující osoby a spoléhající se osoby

Odpovědnost držitele, podepisující osoby a spoléhající se osoby se řídí obecně závaznými právními předpisy.

9.9 Ukončení platnosti smlouvy

Ukončení smlouvy o poskytování certifikačních služeb nebo odstoupení od této smlouvy se řídí Všeobecnými obchodními podmínkami České pošty [VOP].

9.10 Obecné zásady

9.10.1 Komunikační jazyk

Veškerá komunikace mezi zákazníkem (resp. žadatelem) a poskytovatelem certifikačních služeb musí probíhat v českém jazyce, pokud se obě strany nedohodnou jinak.

9.10.2 Použitelnost certifikátů

Certifikáty podle této certifikační politiky jsou vydávány fyzickým osobám, které uzavřely s Českou poštou jednorázovou písemnou smlouvu o poskytování certifikačních služeb. Certifikáty mohou být použity pouze k ověření elektronických podpisů podepisující osoby v souladu se zákonem o elektronickém podpisu [ZoEP].

9.10.3 Povinnosti

9.10.3.1 Povinnosti zákazníka

Fyzická osoba je povinna zejména:

- poskytovat pravdivé a úplné informace při uzavírání smlouvy o poskytování certifikačních služeb,
- poskytovat pravdivé a úplné informace při registraci žádosti o certifikát,
- neprodleně uvědomit poskytovatele certifikačních služeb o změnách údajů, které jsou ve smlouvě uvedeny,
- neprodleně informovat poskytovatele certifikačních služeb o změnách údajů fyzické osoby, které jsou uvedeny v certifikátu. Podle charakteru změny poskytovatel certifikačních služeb rozhodne, zda je třeba revokovat platné certifikáty, které byly pro fyzickou osobu vydány,
- zkontrolovat, zda údaje uvedené v certifikátu jsou správné a odpovídají údajům uvedeným v žádosti,
- 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, který odpovídá veřejnému klíči v certifikátu vydaném podle této certifikační politiky, a odpovídající certifikát 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, a požádat o revokaci certifikátu,

- seznámit se s certifikační politikou, podle které jí byl vydán certifikát,

- zaplatit cenu za vydání certifikátu podle aktuálního platného ceníku.

9.10.3.2 Povinnosti poskytovatele certifikačních služeb

Poskytovatel certifikačních služeb je zejména povinen:

- věnovat náležitou péči všem činnostem spojeným s poskytováním certifikačních služeb; náležitá péče zahrnuje provoz v souladu

  - s provozní dokumentací,

  - s touto certifikační politikou,

  - s certifikační prováděcí směrnicí,

  - systémovou bezpečnostní politikou,

  - platnými právními předpisy,

- do dvou pracovních dnů od podání žádosti posoudit žádost o certifikát, vydat rozhodnutí, zda bude certifikát vydán, a o tomto rozhodnutí informovat fyzickou osobu,

- vydat certifikát vyhovující standardu X.509 a splňující požadavky fyzické osoby,

- vydat certifikát obsahující věcně správné údaje na základě informací, které jsou certifikační autoritě k dispozici v době vydávání certifikátu, bez chyb způsobených registrační autoritou při zadávání údajů,

- informovat fyzickou osobu o tom, že jí byl vydán certifikát, a předat jí vydaný certifikát,

- zveřejnit certifikát do 24 hodin od převzetí certifikátu fyzickou osobou podle pravidel popsaných v odstavci 2.1,

- zneplatnit certifikát podle pravidel popsaných v certifikační politice,

- informovat držitele certifikátu o tom, že jeho certifikát byl zneplatněn z vůle poskytovatele certifikačních služeb nebo orgánu definovaného zákonem o elektronickém podpisu,

- zveřejnit seznam zneplatněných certifikátů do 12 hodin od podání žádosti o zneplatnění certifikátu,

- zveřejňovat certifikační politiky, podle kterých vydává certifikáty, na www serveru poskytovatele certifikačních služeb, případně jinými vhodnými způsoby (viz. odstavec 2.5),

- prověřit podezření, že došlo k prozrazení soukromého klíče v rámci působnosti PostSignum Qualified CA, což by mohlo vést ke ztrátě důvěryhodnosti,

- provádět bezpečnostní audit v souladu s auditní a archivační politikou,

- zveřejnit kvalifikovaný systémový certifikát poskytovatele certifikačních služeb tak, aby se každý mohl ujistit o jeho identitě,

- asistovat při auditu, který provádí externí nebo interní auditor QCA,

- zajistit bezpečný provoz systémů podle požadavků [ZoEP] a navazujících předpisů.

9.10.4 Povinnosti spoléhajících se stran a ostatních uživatelů

Uživatel certifikátu vydaného PostSignum Qualified CA musí zejména:

- Získat certifikáty PostSignum Qualified CA a PostSignum Root QCA z bezpečného zdroje (www server poskytovatele certifikačních služeb, www server orgánu definovaného zákonem o elektronickém podpisu) a ověřit otisk ("fingerprint") těchto certifikátů.

- Před použitím certifikátu vydaného PostSignum Qualified CA ověřit 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.

- Dostatečně zvážit (zejména na základě znalosti příslušné certifikační politiky), zda je certifikát vydaný PostSignum Qualified CA podle této politiky vhodný pro účel, ke kterému jej chce použít.

## 10. PŘÍLOHY – FORMULÁŘE

Tato kapitola popisuje formuláře, které se používají při komunikaci mezi Fyzickou osobou a PostSignum QCA ČP. Aktuální verze formulářů jsou k dispozici na pracovištích registračních autorit nebo na www serveru PostSignum QCA ČP.

### 10.1 Žádost o vydání certifikátu - Politika pro certifikáty určené k ověření elektronického podpisu fyzické osoby

Formulář, který vyplňuje fyzická osoba, pokud chce žádat o certifikát podle této certifikační politiky.

### 10.2 Žádost o zneplatnění certifikátu - Podává fyzická podepisující osoba

Formulář, který vyplňuje držitel certifikátu v případě, že žádá o zneplatnění certifikátu, který byl pro něj vydán.

### 10.3 Žádost o zneplatnění certifikátu - Podává manažer QCA

Formulář, který vyplňuje manažer QCA v případě, že žádá o zneplatnění certifikátu, který byl vydán podle této politiky.

### 10.4 Protokol o vydání a převzetí certifikátu

Protokol, kterým operátor registrační autority stvrzuje vydání certifikátu a držitel potvrzuje převzetí certifikátu.

10.5 **Protokol o zneplatnění certifikátu**

Protokol, kterým se stvrzuje zneplatnění certifikátu.

## 11. LITERATURA

[ZoEP] Zákon 227/2000 Sb. o elektronickém podpisu ve znění pozdějších předpisů

[CPS] Certifikační prováděcí směrnice PostSignum QCA, verze 1.26, vydaná dne 30.6.2005.

[VOP] Všeobecné obchodní podmínky elektronických služeb České pošty, s.p.

[Z101] Zákon 101/2000 Sb. o ochraně osobních údajů ve znění pozdějších předpisů