Certifikační autorita PostSignum VCA České pošty, s.p.

Certifikační politika PostSignum Public CA pro šifrovací certifikáty skupin osob

Verze 1.50

7. listopadu 2005

Česká pošta, s.p.

Schváleno:

Verze	Schválil	
1.30	Komise pro certifikační politiky	e-mail: paa.postsignum@cpost.cz
1.40	Komise pro certifikační politiky	e-mail: paa.postsignum@cpost.cz
1.50	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 VCA vydává více typů certifikátů podle různých politik. Všechny tyto certifikační politiky můžete najít na webových stránkách certifikační autority - www.postsignum.cz.

1.2 Přehled

Česká pošta, s.p. (dále i Česká pošta či ČP) ustanovila certifikační autoritu PostSignum Public CA (dále i PostSignum VCA), které vydala certifikát certifikační autorita PostSignum Root QCA. PostSignum Public CA vydává 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 VCA, 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 pracoviště registrační autority 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.

Certifikáty veřejného klíče vydané podle této certifikační politiky jsou určeny pro skupiny osob, které jsou v určitém vztahu k zákazníkovi, který uzavírá s Českou poštou smlouvu o poskytování certifikačních služeb. Skupina se skládá z členů skupiny. Zákazník (prostřednictvím oprávněné osoby) definuje, pro které skupiny osob mají být certifikáty vydány. Zákazník rovněž stanoví, kdo bude danou skupinu reprezentovat vůči PostSignum Public CA, tedy kdo smí být žadatelem o certifikát podle této politiky. Žadatelé zastupují skupinu při jednání s PostSignum Public CA, zejména při registraci žádosti o certifikát a žádosti o revokaci certifikátu. Držitelem certifikátu je zákazník České pošty.

Zákazník odpovídá za vazbu mezi údaji o sobě, které jsou v certifikátu uvedeny. Poskytovatel certifikačních služeb ověřuje vazbu mezi žadatelem o certifikát a veřejným klíčem v certifikátu.

Certifikáty vydané podle této certifikační politiky mohou být použity zajištění služby šifrování.

Zákazník uzavře s Českou poštou písemnou smlouvu o poskytování certifikačních služeb tak, jak je v obchodním styku obvyklé. Smlouva mimo jiné obsahuje údaje o oprávněných osobách, které smějí definovat, kterým skupinám mají být vydány certifikáty podle této certifikační politiky. Oprávněná osoba doručí České poště seznam žadatelů o certifikát, pro které mají být vydány certifikáty podle této certifikační politiky, spolu s případnými omezeními, pro které skupiny mohou žadatelé žádat. Žadatel o certifikát se osobně dostaví na pracoviště registrační autority PostSignum Public CA, kde předloží jeden osobní doklad a digitální žádost o certifikát. Pokud je žadatel o certifikát uveden v seznamu žadatelů dodaném oprávněnou osobou a pokud je jeho osobní doklad v pořádku, je mu vydán certifikát s veřejným klíčem z digitální žádosti a s údaji,

které odpovídají údajům uvedeným v seznamu žadatelů. Žadatel o certifikát zkontroluje údaje uvedené v certifikátu a pokud s nimi souhlasí, písemně potvrdí převzetí certifikátu. Tímto okamžikem se zákazník České pošty stává držitelem certifikátu.

Členové skupiny, kteří nejsou žadatelem, sice mají právo disponovat soukromým klíčem odpovídajícím veřejnému klíči uvedenému v certifikátu, ale nemohou žádat o vydání a zneplatnění certifikátu dané skupiny.

Plnění zásad této politiky rozpracovává a zajišťuje aktuální Certifikační prováděcí směrnice PostSignum VCA, verze 1.30 a vyšší.

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

1.2.1 Certifikační služby poskytované PostSignum Public CA

Certifikační autorita PostSignum Public 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 VCA,
- informace o poskytovaných službách.

1.3 Identifikace politiky

Tab. 1 Identifikace politiky

Název politiky	Politika pro šifrovací certifikáty skupin osob
Verze politiky	1.50
Stav	Finální
OID poskytovatele certifikačních služeb	2.23.134
OID PostSignum Root QCA	2.23.134.1.4.2.1
OID PostSignum Public CA	2.23.134.1.2.2.3
OID této politiky	2.23.134.1.2.1.2.150
Datum vydání	7.11.2005
Doba platnosti	do odvolání
Odpovídající CPS	Aktuální Certifikační prováděcí směrnice PostSignum VCA, verze 1.30 a vyšší

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 vydala certifikát pro certifikační autoritu PostSignum Public CA. Jejím úkolem je především vydávat a spravovat certifikáty certifikačních autorit působících v rámci České pošty.

1.4.3 PostSignum Public CA

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

1.4.4 Registrační autority

Žadatelé o certifikát, kteří 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 žadatelů o certifikát, poté přijmout nebo zamítnout žádost a předat vydaný certifikát žadateli. Na pracovišti registrační autority je možné podat žádost o zneplatnění certifikátu.

1.4.5 Klienti PostSignum Public CA

Klientem PostSignum Public CA je v případě certifikátu vydaného podle této certifikační politiky osoba, která je v určitém vztahu se zákazníkem České pošty.

1.5 Oblast použití

PostSignum Public CA vydává certifikáty určené k ověření elektronických podpisů, autentizaci a šifrování dat jak pro organizace, které požadují větší počet certifikátů, tak pro jednotlivce.

Certifikáty vydané podle této certifikační politiky mohou být použity pouze k zajištění služeb šifrování dat určených pro členy této skupiny.

Certifikáty vydávané PostSignum Public CA podle této politiky jsou vhodné pro použití v aplikaci REP (Registrovaná elektronická pošta).

1.5.1 Omezení použití certifikátu

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

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 prováděcí směrnice odpovídá manažer VCA.

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. Jedná se jak o politiky pro kořenovou certifikační autoritu (PostSignum Root QCA), tak o politiky pro podřízené certifikační autority, tedy i PostSignum Public CA.

1.6.3 Správa dokumentu

Tento dokument je vytvářen týmem pro tvorbu certifikačních politik ČP (Policy Creation Authority - PCA PostSignum), který je dále zodpovědný za tvorbu certifikačních politik. PCA PostSignum je dle potřeby ustavován Komisí pro certifikační politiky ČP, je jí řízen a kontrolován. PCA PostSignum 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 VCA (např. změně postupů), která ovlivní obsah těchto dokumentů,
- pokud při pravidelné kontrole okolního prostředí PostSignum VCA 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 VCA. 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 webových stránkách PostSignum Public CA. 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 Public 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 VCA, 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 VCA. Kontaktní adresa manažera VCA 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

Webové stránky certifikační autority PostSignum Root QCA mají 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 Public CA

Webové stránky certifikační autority PostSignum Public CA mají adresu:

http://www.postsignum.cz

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

ldap://vca.postsignum.cz

1.7.7 Registrační autority

Aktuální seznam registračních autorit je k dispozici na webových stránkách PostSignum VCA.

1.7.8 Kontaktní osoba

Kontaktní osobou pro PostSignum Public CA je manažer VCA. 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 VCA, jehož adresa je:

manager.postsignum@cpost.cz

1.8 Použité zkratky a pojmy

VCA - viz. PostSignum Public CA

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].

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

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

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

Obchodní místo - centrální regionální pracoviště odpovědné za uzavírání a evidenci smluv.

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

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

Rozlišovací jméno - jednoznačně identifikuje osobu dle pravidel definovaných příslušnou certifikační politikou.

Správa žadatelů - aplikace VCA 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 Public 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 VCA rozlišuje dva typy zákazníků: **zákazník - organizace** a **zákazník - fyzická osoba**.

Žadatel - osoba, která má právo žádat u PostSignum Public 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 na webových stránkách PostSignum VCA.

Prostřednictvím adresářového serveru i webových stránek 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://vca.postsignum.cz

CRL je zveřejňován rovněž na adrese

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

2.3 Zveřejňování informací o certifikační autoritě

Certifikační autorita PostSignum Public CA zveřejňuje své certifikační politiky na webových stránkách PostSignum VCA.

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 Public CA, u nichž byl vysloven souhlas se zveřejněním, jsou zveřejňovány elektronickou cestou nejpozději do 24 hodin od převzetí certifikátu žadatelem (viz odstavec 4.5).

Seznamy zneplatněných certifikátů (CRL) jsou zveřejňovány alespoň jednou za dvanáct hodin. V případě zneplatnění certifikátu vydaného PostSignum Public 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 webových stránkách PostSignum VCA 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 se zákazníkem

Zákazník uzavírající smlouvu o poskytování certifikačních služeb prokazuje svou totožnost tak, jak je v obchodním styku obvyklé.

3.2 Změna oprávněné osoby

V době platnosti smlouvy může dojít ke změně ve jmenování oprávněných osob. Změna musí být zachycena v dodatku smlouvy, kde bude uvedena nová oprávněná osoba a její podpisový vzor.

3.3 Pre-Registrace žádosti o certifikát

Oprávněná osoba stvrzuje svým podpisem správnost seznamů žadatelů o certifikát. Podpis oprávněné osoby je na České poště kontrolován oproti podpisovému vzoru, který je součástí smlouvy mezi zákazníkem a Českou poštou.

3.4 Registrace žádostí o certifikát

Žadatel o certifikát prokazuje svou totožnost platným občanským průkazem nebo platným cestovním pasem v případě občana České republiky, respektive platným cestovním pasem nebo řidičským průkazem Evropské unie v případě občana jiného státu. Pracovník registrační autority zkontroluje:

- zda je doklad platný,
- zda fotografie na dokladu odpovídá žadateli o certifikát,
- zda údaje z dokladu odpovídají údajům uvedeným v seznamu žadatelů.

Žádost je zaregistrována pouze tehdy, pokud jsou splněny všechny výše uvedené podmínky.

3.5 Registrace žádostí o zneplatnění certifikátů

O zneplatnění certifikátu může žádat žadatel nebo oprávněná osoba. Žadatel prokáže svou totožnost:

- znalostí hesla pro zneplatnění, které zadal při registraci žádosti o certifikát, nebo
- osobním dokladem obdobně jako při registraci žádosti o certifikát.

Oprávněná osoba se prokáže svým podpisem obdobně jako při předání seznamu žadatelů.

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

3.6 Registrace žádostí o obnovu certifikátu

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

3.7 Znakové sady a transkripce údajů

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

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

Veškeré údaje dokladované oprávněnou osobou při pre-registraci žádosti o certifikát se do certifikátů vydávaných PostSignum Public CA a do žádostí o certifikáty přenášejí buď:

- ve tvaru, ve kterém jsou uvedeny v předkládaných dokladech (transkripce, jako například odstranění diakritiky, není možná) nebo:

- ve tvaru, který je kódován znakovou sadou neobsahující české znaky a je přesnou transkripcí bez diakritiky údajů v předkládaných dokladech.

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

3.8 Jednoznačnost jmen

Zákazník ručí za jednoznačnost jmen skupin v rámci zákazníka. V položce Subject certifikátu je uvedena kombinace jednoznačných údajů o zákazníkovi (IČ zákazníka a jméno zákazníka) a jednoznačných údajů o skupině, čímž je zaručeno, že dvěma různým skupinám nebudou vydány certifikáty se stejnou položkou Subject

3.9 Pseudonym

PostSignum Public CA nepodporuje zákazníka v položce Subjekt certifikátu.

3.10 E-mailová adresa

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

3.11 Postup v případě kolize jmen

V případě kolize rozlišovacích jmen dvou žadatelů o certifikát, a tím i kolize položky Subject v certifikátech těchto dvou osob, rozhodne o řešení manažer VCA a toto řešení navrhne oprávněným osobám zákazníků do dvou pracovních dní od vzniku kolize.

4. PROVOZNÍ POŽADAVKY

4.1 Uzavření smlouvy

Zákazník získá přístup ke službě poskytování certifikačních služeb uzavřením písemné smlouvy o poskytování certifikačních služeb (smlouva o poskytování služeb). Tato smlouva se uzavírá následujícím způsobem:

Zákazník zašle vyplněnou objednávku na poskytování certifikačních služeb (Objednávka služeb) podle formulářů, které jsou k dispozici na webové stránce poskytovatele, a ČP akceptuje objednávku služeb zákazníka.

Formuláře pro objednávku certifikačních služeb obsahují odkazy na webové stránky, na nichž je možno získat Certifikační politiky, CPS a aktuální ceník.

Certifikační politika a aktuální ceník se stávají součástí smlouvy o poskytování služeb spolu s VOP (Všeobecnými obchodními podmínkami elektronických služeb České pošty) a akceptovanou objednávkou služeb ke dni uzavření smlouvy o poskytování služeb.

Objednávka certifikačních služeb obsahuje mimo jiné:

- identifikační údaje zákazníka včetně IČ a případně rozšířeného IČ,
- typy požadovaných certifikačních služeb,
- seznam oprávněných osob, které budou s poskytovatelem certifikačních služeb komunikovat ohledně vydávání certifikátů,
- podpisové vzory oprávněných osob.

Objednávka je zákazníkem podepsána tak, jak je v obchodním styku obvyklé (statutární zástupce organizace apod.), a stává se součástí smlouvy o poskytování certifikačních služeb. Objednávka musí být v písemné formě.

Česká pošta si vyhrazuje právo nepřistoupit k uzavření smlouvy o poskytování certifikačních služeb.

4.2 Pre-registrace žadatelů o certifikát

Pre-registrací se rozumí postup, kdy oprávněná osoba schvaluje seznam žadatelů, kteří mohou žádat o certifikát podle této certifikační politiky, a tento seznam předává poskytovateli certifikačních služeb.

O každém žadateli o certifikát musí být uvedeny alespoň tyto údaje:

- jméno a příjmení, případně tituly,
- pro občany ČR rodné číslo, pro cizince datum narození,
- jednoznačné číslo žadatele v organizaci.

Volitelně mohou být uvedena omezení, pro které technologické komponenty má žadatel právo žádat o certifikát. Tato omezení mohou zahrnovat kterékoliv z následujících omezení nebo obě omezení zároveň:

- označení organizační jednotky, které musí být uvedeno v označení skupiny v položce Subject certifikátu,
- jméno skupiny, které musí být uvedeno v označení skupiny v položce Subject certifikátu.

Pokud nejsou uvedena žádná omezení, žadatel může žádat o certifikát pro jakoukoliv skupinu v rámci organizace zákazníka.

Kromě seznamu žadatelů oprávněná osoba též schvaluje seznam skupin, pro které se bude žádat o certifikát. Pro každou skupinu jsou uvedeny tyto údaje:

- organizační jednotka, kde skupina působí (nepovinná položka),
- název skupiny (povinná položka),
- e-mailová adresa skupiny (nepovinná položka),
- příznak zveřejnění resp. nezveřejnění vydaného certifikátu široké veřejnosti bez omezení

Některé z uvedených údajů jsou mapovány do položek uvedených v certifikátu, jak je uvedeno v Tab. 2.

Tab.2 Mapování údajů

Požadovaný údaj	**Údaj v certifikátu**
IČ a název zákazníka	Položka Subject, atribut O
Jméno a příjmení žadatele	V certifikátu neuvedeno
Rodné číslo nebo datum narození	V certifikátu neuvedeno
Jednoznačné číslo žadatele	V certifikátu neuvedeno
Organizační jednotka, kde skupina působí	Položka Subject, atribut OU
Název skupiny	Položka Subject, atribut CN
Adresa elektronické pošty	Rozšíření SubjectAltName

Registrační autorita PostSignum Public CA ověřuje totožnost žadatele o certifikát pomocí standardních dokladů - občanských průkazů a cestovních pasů. Protože v certifikátu jsou uváděny rovněž údaje o zákazníkovi, ke kterému žadatel o certifikát patří, pracovník registrační autority PostSignum Public CA musí ověřit i tuto vazbu.

Proto jsou ve smlouvě o poskytování certifikačních služeb definovány oprávněné osoby, které poskytovateli certifikačních služeb garantují vazbu mezi žadatelem o certifikát a zákazníkem. Oprávněné osoby musí provést pre-registraci žadatelů, kteří mohou u PostSignum Public CA žádat o certifikát. Pokud přestane být v zájmu zákazníka, aby žadatel mohl žádat o certifikát, oprávněná osoba oznámí poskytovateli certifikačních služeb tuto změnu, případně požádá o revokaci certifikátů, které byly pro daného žadatele vydány.

4.3 Registrace žádosti o certifikát a vydání certifikátu

Žadatel o certifikát se dostaví na pracoviště registrační autority, kde předloží jeden osobní doklad 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 žadatel o certifikát v době vytváření žádosti vlastnil soukromý klíč odpovídající veřejnému klíči uvedenému v žádosti.

Pracovník registrační autority zkontroluje osobní doklad. Oproti seznamu žadatelů ověří, zda daná osoba skutečně smí žádat o certifikát dle dané certifikační politiky a zda údaje v digitální žádosti souhlasí s údaji v seznamu žadatelů. Pokud údaje v digitální žádosti nesouhlasí s údaji uvedenými v seznamu žadatelů, pracovník registrační autority opraví údaje tak, aby byly v souladu s údaji uvedenými v seznamu žadatelů. Pokud žadatel o certifikát s takovou úpravou nesouhlasí, není mu vydán certifikát. Žadatel o certifikát při registraci zadává rovněž heslo, pomocí kterého bude certifikát v případě potřeby zneplatňovat.

Pokud jsou všechny údaje v pořádku, pracovník registrační autority schválí vydání certifikátu.

Pokud má pracovník registrační autority pochybnosti o předloženém dokladu nebo pokud se vyskytnou jiné nesrovnalosti, odmítne vydat certifikát a o této skutečnosti informuje jak žadatele o certifikát, tak příslušnou oprávněnou osobu.

4.4 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.

4.5 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 o certifikát za zákazníka 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.

Vydaný certifikát je žadateli předán ve formátu DER spolu s certifikátem vydávající certifikační autority PostSignum Public CA a s certifikátem kořenové certifikační autority PostSignum Root QCA. Certifikáty autorit jsou rovněž ve formátu DER.

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

4.6 Obnova certifikátu

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

4.7 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 Public CA znovu použity.

4.8 Zneplatnění certifikátu

4.8.1 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,
- příslušná žádost držitele nebo žadatele.

4.8.2 Osoby oprávněné žádat o zneplatnění certifikátu

O zneplatnění certifikátu může požádat držitel certifikátu prostřednictvím oprávněné osoby, žadatel o certifikát nebo manažer certifikační autority, která vydala certifikát.

4.8.3 Postup zneplatnění na žádost držitele certifikátu

4.8.3.1 Žádost o zneplatnění certifikátu podaná osobně žadatelem na registrační autoritě

Žadatel požádá o zneplatnění certifikátu osobně na pracovišti 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 žadatele v evidenci žadatelů o certifikát a ověří jeho 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 žadateli protokol o zneplatnění certifikátu. Žadatel protokol podepíše.

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

Žadatel podává žádost o zneplatnění certifikátu telefonicky, písemně nebo faxem na telefonní číslo nebo adresu uvedenou v certifikační politice nebo jiným vzdáleným způsobem specifikovaným na webových stránkách PostSignum VCA. 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 žadatelem.

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 žadatele (a zákazníka).

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

4.8.4 Žádost o zneplatnění certifikátu podaná oprávněnou osobou

V případě, že o zneplatnění žádá zákazník, učiní tak písemnou formou. Žádost o zneplatnění je podepsaná oprávněnou osobou.

Po úspěšném zneplatnění je vytvořen protokol o zneplatnění certifikátu, který je neprodleně zaslán zákazníkovi. Zákazník je o zneplatnění certifikátu informován rovněž prostřednictvím elektronické pošty, pokud oprávněná osoba vlastní certifikát vydaný PostSignum Public CA, ve kterém je uvedena její e-mailová adresa.

4.8.5 Zneplatnění certifikátu z vůle certifikační autority

O revokaci certifikátu může rozhodnout rovněž poskytovatel certifikačních služeb, pokud žadatel nebo zákazník porušují pravidla certifikační politiky nebo dohodnuté smluvní podmínky. PostSignum VCA v takovém případě informuje zákazníka o zneplatnění certifikátu s udáním důvodu, proč byl certifikát revokován. Manažer VCA 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 oprávněná osoba vlastní certifikát vydaný PostSignum Public CA, ve kterém je uvedena její e-mailová adresa.

4.8.6 Časová prodleva od přijetí žádosti o zneplatnění

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

4.9 Informace o stavu certifikátu

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

- na webových stránkách PostSignum VCA,
- v adresářových službách PostSignum VCA,
- u nezávislého poskytovatele webových.

Primárním zdrojem aktuálního CRL jsou webové stránky PostSignum VCA.

PostSignum Public CA neposkytuje informace o stavu certifikátu protokolem OCSP.

4.11 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, dojde k přirozenému ukončení jeho platnosti. 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 webových stránkách a adresářovém serveru PostSignum VCA.

5. BEZPEČNOST FYZICKÁ, PROCEDURÁLNÍ A PERSONÁLNÍ

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

5.1 Ukončení činnosti PostSignum Public CA

Ukončení činnosti PostSignum Public CA musí být písemně oznámeno všem držitelům platných certifikátů a rovněž zveřejněno na webových stránkách PostSignum VCA uvedeném v kapitole 1.7.6 a na všech pracovištích registrační autority PostSignum VCA. Součástí oznámení musí být i informace o ukončení platnosti certifikátu autority včetně příslušného důvodu ukončení. Dokud je platný alespoň jeden certifikát vydaný PostSignum Public CA, musí PostSignum Public CA zajišťovat alespoň funkci zneplatnění certifikátu a vydání CRL.

Pokud PostSignum Public 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 Public CA zneplatní všechny dosud platné vydané certifikáty a vydá poslední CRL. Teprve poté může být činnost PostSignum Public CA ukončena.

Zneplatněný kvalifikovaný systémový certifikát PostSignum Public 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 Public CA, která sloužila pro podepisování certifikátů a seznamů zneplatněných certifikátů.

5.1.1 Podezření na kompromitaci soukromého klíče PostSignum Public CA

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

PostSignum Root QCA okamžitě zneplatní certifikát PostSignum Public 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 Public CA.

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

6. TECHNICKÁ BEZPEČNOST

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

6.1 Ochrana klíčů autority

Soukromý klíč PostSignum Public 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 žadatelů o certifikát jsou generovány a uschovávány žadatelem. Jedná se o klíče pro algoritmus RSA, s délkou 1024 nebo 2048 bitů. PostSignum Public CA s těmito klíči nepřichází do styku, není zodpovědná za jejich ochranu ani zálohování.

Obecně je však možné držitelům certifikátů a žadatelům o certifikát 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. 3 Profil certifikátu

Version	3 (0x2)
Serial Number	*PostSignum Public CA přiřazuje každému vydanému certifikátu jednoznačné číslo.*
SignatureAlgorithm	sha1WithRSAEncryption
Issuer	
Country	CZ
Organisation	Česká pošta, s.p. [IČ 47114983] *uvedené číslo je IČ České pošty, s.p.*
CN	PostSignum Public CA
Validity	
Not Before	*Datum vydání - UTCTime*
Not After	*1 rok od data vydání - UTCTime*
Subject	
Country	CZ
Organisation	*Název zákazníka - držitele certifikátu* [IČ *xxxxxxxx*] *xxxxxxxx je IČ zákazníka včetně rozšíření IČ, pokud bylo uvedeno - údaj ze žádosti*
OU	groups
OU	*Nepovinná položka, organizační jednotka, kde působí skupina, pro kterou je vydán certifikát* *- údaj ze žádosti*
CN	*Identifikace skupiny*
Subject Public Key Info	
Algorithm	rsaEncryption
SubjectPublicKey	*veřejný klíč*
Extensions	*rozšíření certifikátu podle tabulky 4*
Signature	*elektronická značka poskytovatele certifikačních služeb*

Položka Subject certifikátu jednoznačně identifikuje skupinu osob.

Tab. 4 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
Key Usage		ano
DigitalSignature	ne	
NonRepudiation	ne	
KeyEncipherment	ano	
DataEncipherment	ne	
KeyAgreement	ne	
KeyCertSign	ne	
CRLSign	ne	
CertificatePolicies		ne
Policy Identifier	2.23.134.1.2.1.2.150	
Policy Qualifier id	CPS	
CPS URI	http://www.postsignum.cz	
CRL Distribution Points	URI: http://www.postsignum.cz/crl/pspublicca.crl URI: http://postsignum.ttc.cz/crl/pspublicca.crl URI: ldap://vca.postsignum.cz/cn=PostSignum Public CA,o=Ceska posta s.p. [IC 47114983],c=CZ	ne
Basic Constraints	cA:FALSE	ne

Tab. 5 Profil CRL

Version	2 (0x1)
Issuer Distinguished Name	
Country	CZ
Organisation	Česká pošta, s.p. [IČ 47114983]
CN	PostSignum Public 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 6*
CrlExtensions	*rozšíření CRL podle tabulky 6*
SignatureAlgorithm	sha1WithRSAEncryption
Signature	*elektronická značka poskytovatele certifikačních služeb*

Tab. 6 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 Public 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. 7 Profil žádosti o certifikát

Položka	Obsah	Poznámka
Subject		
Country	CZ	
Organisation	*Název zákazníka - držitele certifikátu* [IČ *xxxxxxxx*] *xxxxxxxx je IČ organizace včetně rozšíření IČ, pokud je uvedeno*	
Organisation Unit	Groups	Určuje typ certifikátu
Organisation Unit	*Nepovinná položka, organizační jednotka, kde působí skupina, pro kterou je vydán certifikát*	Pokud má být v certifikátu uvedeno.
CN	*Identifikace skupiny*	
Extensions		
SubjectAltName	*E-mailová adresa*	Pokud má být v certifikátu uvedeno. Rozšíření certifikátu.

8. HODNOCENÍ SHODY A SOULADU S PŘEDPISY

8.1 Audit a kontrola

Činnost PostSignum VCA podléhá auditu a kontrole. Audit a kontroly PostSignum VCA provádí pracovníci České pošty, s.p., jednou ročně je provoz PostSignum Public CA prověřen externím auditorem nezávislým na České poště, s.p.

8.2 Oblasti auditu a kontroly

Oblasti hodnocené v rámci pravidelných kontrol, interních a externích auditů jsou specifikovány v Certifikační prováděcí směrnici.

8.3 Opatření v případě zjištění nedostatků

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

8.4 Archivace záznamů

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

8.4.1 Typy uchovávaných archivních záznamů

V PostSignum VCA 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 VCA a záznamy o školení obsluhy,
- logy automaticky vytvářené komponentami informačního systému PostSignum VCA.

9. DALŠÍ OBCHODNÍ A PRÁVNÍ ZÁSADY

9.1 Poplatky za služby

Cena za poskytnuté certifikační služby je stanovena ve smlouvě mezi zákazníkem a poskytovatelem certifikačních služeb a řídí se aktuálním platným ceníkem. Cena za vydané certifikáty může být i zahrnuta v ceně jiné služby poskytované Českou poštou.

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.

Výroční zpráva je k nahlédnutí též na webových stránkách 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 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 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, žadatelům o certifikát nebo spoléhajícím se osobám, jakož i auditorům pro účely vyjádření shody - auditu dle odst. 2.7 výše, a dále poskytuje informace 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 VCA.

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

9.4.2 Zpřístupnění osobních údajů orgánům zmocněným ze zákona

Veškeré informace zpracovávané v PostSignum VCA 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 VCA poté, co orgány zmocněné ze zákona prokáží své zmocnění způsobem obvyklým v těchto případech.

9.4.3 Zpřístupnění informací na základě požadavku klienta

PostSignum VCA poskytuje klientovi v souladu se zákonem [Z101] informace o osobních údajích, které PostSignum VCA 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 VCA a ke struktuře, organizaci, vzhledům obrazovek a obsahu webových stránek PostSignum VCA.

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 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 VCA.

c) Česká pošta neodpovídá za škodu vyplývající z použití certifikátu v období po přijetí žádosti o jeho zneplatnění, pokud Česká pošta dodrží lhůtu pro zveřejnění zneplatněného 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, členů skupin a spoléhající se osoby

Odpovědnost držitele, členů skupin 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 vydané podle této certifikační politiky mohou být použity pouze k šifrování dat určených pro členy této skupiny.

9.10.3 Povinnosti

9.10.3.1 Povinnosti zákazníka

Zákazník je povinen zejména:

- poskytovat pravdivé a úplné informace při uzavírání smlouvy o poskytování certifikačních služeb,
- neprodleně uvědomit poskytovatele certifikačních služeb o změnách údajů, které jsou ve smlouvě uvedeny, zejména o změnách údajů o oprávněných osobách,
- neprodleně informovat poskytovatele certifikačních služeb o změnách údajů zákazníka, které jsou uvedeny v certifikátu. Podle charakteru změny poskytovatel certifikačních služeb rozhodne, zda je třeba revokovat platné certifikáty, které byly pro zákazníka vydány,
- zaplatit cenu za vydání certifikátu podle aktuálního ceníku.

9.10.3.2 Povinnosti oprávněných osob

Oprávněná osoba je povinna zejména:

- poskytovat pravdivé a úplné informace o žadatelích oprávněných žádat o certifikát podle této politiky,
- neprodleně uvědomit poskytovatele certifikačních služeb o změnách údajů, které udržuje v seznamech žadatelů o certifikát,
- zajistit, že číslo přiřazené žadateli o certifikát bude v rámci zákazníka jednoznačné.

Oprávněná osoba dále definuje, které certifikáty zákazníka budou zveřejněny prostřednictvím informačních služeb poskytovatele certifikačních služeb. Tyto služby jsou přístupné široké veřejnosti bez omezení.

9.10.3.3 Povinnosti žadatele o certifikát

Žadatel o certifikát je povinen zejména:

- poskytovat pravdivé a úplné informace při registraci žádosti o certifikát,
- 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 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, a požádat o revokaci certifikátu,

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

9.10.3.4 Povinnosti členů skupiny

Člen skupiny je povinen:

- užívat soukromý klíč a certifikát pouze pro účely stanovené v certifikační politice,

- nakládat se soukromým klíčem s náležitou péčí, a to tak, aby nemohlo dojít k jeho neoprávněnému použití,

- uvědomit žadatele neprodleně o skutečnostech, které vedou ke zneplatnění certifikátu, zejména o podezření, že soukromý klíč byl zneužit; žadatel poté požádá o zneplatnění certifikátu.

Soukromý klíč nesmí být použit k jiným účelům, než

- k dešifrování dat určených členům skupiny.

9.10.3.5 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 žadatele nebo zákazníka,

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

- 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 žadatele o certifikát o tom, že mu byl vydán certifikát, a předat mu vydaný certifikát,

- zveřejnit certifikát do 24 hodin od převzetí certifikátu žadatelem 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,
- zveřejnit seznam zneplatněných certifikátů do 12 hodin od přijetí žádosti o zneplatnění certifikátu,
- zveřejňovat certifikační politiky, podle kterých vydává certifikáty, na webových stránkách PostSignum VCA, případně jinými vhodnými způsoby (viz. odstavec 2.3),
- prověřit podezření, že došlo k prozrazení soukromého klíče v rámci působnosti PostSignum Public 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 kontrole nebo auditu, který provádí externí auditor nebo pověřený pracovník České pošty.

9.10.4 Povinnosti spoléhajících se stran a ostatních uživatelů

Uživatel certifikátu vydaného PostSignum Public CA musí zejména:

- Získat certifikáty PostSignum Public CA a PostSignum Root QCA z bezpečného zdroje (webové stránky PostSignum VCA) a ověřit otisk ("fingerprint") těchto certifikátů.
- Před použitím certifikátu vydaného PostSignum Public CA ověřit platnost certifikátu PostSignum Public 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 Public 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 zákazníkem a PostSignum VCA. Aktuální verze formulářů jsou k dispozici na pracovištích registračních autorit nebo na webových stránkách PostSignum VCA.

10.1 **Seznam žadatelů - Politika pro šifrovací certifikáty skupin osob**

Formulář, který schvaluje (a případně vyplňuje) oprávněná osoba. Obsahuje seznam žadatelů, kteří smějí žádat o certifikát podle této politiky.

10.2 **Změny v seznamu žadatelů - Politika pro šifrovací certifikáty skupin osob**

Formulář, který schvaluje (a případně vyplňuje) oprávněná osoba. Používá se tehdy, pokud je třeba změnit údaje o žadatelích o certifikát, které vede poskytovatel certifikačních služeb v seznamu žadatelů.

10.3 **Žádost o zneplatnění certifikátu - Podává žadatel o certifikát**

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

10.4 **Žádost o zneplatnění certifikátu - Podává oprávněná osoba jakožto zástupce zákazníka**

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

10.5 **Žádost o zneplatnění certifikátu - Podává manažer VCA**

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

10.6 **Protokol o vydání a převzetí certifikátu**

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

10.7 **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] Aktuální Certifikační prováděcí směrnice PostSignum VCA, verze 1.30 a vyšší

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

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