

Certifikační autorita PostSignum VCA České pošty, s.p.

**Certifikační politika PostSignum Public CA
pro komerční serverové certifikáty**

Verze 1.1

30. ledna 2010

Česká pošta, s.p.

**Certifikační politika PostSignum Public CA
pro komerční serverové certifikáty verze 1.1**

Schváleno:

Verze	Schválil	
1.0	Komise pro certifikační politiky	e-mail: paa.postsignum@cpost.cz
1.1	Komise pro certifikační politiky	e-mail: paa.postsignum@cpost.cz

1 Úvod	5
1.1 Přehled.....	5
1.2 Název a jednoznačné určení dokumentu	6
1.3 Participující subjekty	6
1.4 Použití certifikátu	10
1.5 Správa politiky	10
1.6 Přehled použitých pojmů a zkratk	11
2 Odpovědnost za zveřejňování a úložiště informací a dokumentace.....	14
2.1 Úložiště informací a dokumentace	14
2.2 Zveřejňování informací a dokumentace	14
2.3 Periodicita zveřejňování informací	15
2.4 Řízení přístupu k jednotlivým typům úložišť.....	15
3 Identifikace a autentizace	16
3.1 Pojmenování.....	16
3.2 Počáteční ověření identity	17
3.3 Identifikace a autentizace při zpracování požadavků na výměnu veřejného klíče v certifikátu	19
3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu	19
4 Požadavky na životní cyklus certifikátu.....	21
4.1 Žádost o vydání certifikátu.....	21
4.2 Zpracování žádosti o certifikát	23
4.3 Vydání certifikátu.....	24
4.4 Převzetí vydaného certifikátu	24
4.5 Použití párových dat a certifikátu.....	25
4.6 Obnovení certifikátu.....	26
4.7 Výměna veřejného klíče v certifikátu	26
4.8 Změna údajů v certifikátu	29
4.9 Zneplatnění a pozastavení platnosti certifikátu	30
4.10 Služby související s ověřováním statutu certifikátu	33
4.11 Ukončení poskytování služeb pro držitele certifikátu.....	33
4.12 Úschova soukromého klíče u důvěryhodné třetí strany a jejich obnova.....	34
5 Management, provozní a fyzická bezpečnost	35
5.1 Fyzická bezpečnost	35
5.2 Procesní bezpečnost	36
5.3 Personální bezpečnost	37
5.4 Auditní záznamy (logy).....	38
5.5 Uchovávání informací a dokumentace	39
5.6 Výměna dat pro ověřování elektronických značek v nadřízeném komerčním systémovém certifikátu poskytovatele	40
5.7 Obnova po havárii nebo kompromitaci	40
5.8 Ukončení činnosti CA nebo RA	42
6 Technická bezpečnost.....	44
6.1 Generování a instalace párových dat.....	44
6.2 Ochrana soukromého klíče a bezpečnost kryptografických modulů.....	45
6.3 Další aspekty správy párových dat.....	47

6.4 Aktivační data	47
6.5 Počítačová bezpečnost.....	47
6.6 Bezpečnost životního cyklu	48
6.7 Síťová bezpečnost	48
6.8 Časová razítka	48
7 Profily certifikátu, seznamu zneplatněných certifikátů a OCSP.....	49
7.1 Profil certifikátu	49
7.2 Profil seznamu zneplatněných certifikátů	51
7.3 Profil OCSP.....	52
8 Hodnocení shody a jiná hodnocení	53
8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení	53
8.2 Identita a kvalifikace hodnotitele	53
8.3 Vztah hodnotitele k hodnocenému subjektu	53
8.4 Hodnocené oblasti	53
8.5 Postup v případě zjištění nedostatků	53
8.6 Sdělování výsledků hodnocení.....	53
9 Ostatní obchodní a právní záležitosti	54
9.1 Poplatky.....	54
9.2 Finanční odpovědnost	54
9.3 Citlivost obchodních informací	54
9.4 Ochrana osobních údajů	55
9.5 Práva duševního vlastnictví.....	56
9.6 Zastupování a záruky	56
9.7 Zřeknutí se záruk	57
9.8 Omezení odpovědnosti	57
9.9 Odpovědnost za škodu, náhrada škody	57
9.10 Doba platnosti, ukončení platnosti	57
9.11 Komunikace mezi zúčastněnými subjekty	58
9.12 Změny.....	58
9.13 Řešení sporů	59
9.14 Rozhodné právo.....	59
9.15 Shoda s právními předpisy	59
9.16 Další ustanovení	59
9.17 Další opatření	60

1 ÚVOD

Tento dokument stanoví pravidla a postupy pro vydávání komerčních serverových certifikátů. Pověřená osoba organizace (nebo přímo samotný zákazník v případě podnikající nebo nepodnikající fyzické osoby) stanoví, které osoby mohou o vydání certifikátu žádat.

1.1 Přehled

Česká pošta, s.p. (dále i Česká pošta či ČP) ustavila dvouúrovňovou hierarchii certifikačních autorit s názvem PostSignum VCA. Kořenem této hierarchie je PostSignum Root QCA, která vydala certifikát pro certifikační autoritu PostSignum Public CA. PostSignum Public CA vydává komerční certifikáty a komerční systémové certifikáty koncových uživatelů, přičemž uplatňuje model tzv. pre-registrace zákazníka, jehož cílem je minimalizovat účast statutárního zástupce organizace v celém procesu a vyžadovat minimální množství dokladů od osob, jež si budou žádat o certifikát.

Zákazník, který má zájem o služby PostSignum VCA, uzavře s Českou poštou smlouvu o poskytování certifikačních služeb. Ve smlouvě jsou stanoveny tzv. pověřené osoby, které jménem zákazníka stanovují, kterým žadatelům budou moci být vydány certifikáty podle jednotlivých certifikačních politik. Tito žadatelé jsou zavedeni do systému certifikační autority a následně požádají o certifikát na registrační autoritě České pošty.

V případě podnikajících fyzických osob bez zaměstnanců (podnikatelů) a nepodnikajících fyzických osob (občanů) je pověřenou osobou i žadatelem o certifikát přímo samotný zákazník a proces pre-registrace je zjednodušen. Uzavření smlouvy a vydání certifikátu může proběhnout při jedné návštěvě registrační autority.

Česká pošta může dohodnout se zákazníkem zvláštní podmínky procesu registrace, případně vznik nové certifikační politiky.

Komerční certifikáty veřejného klíče vydané podle této certifikační politiky jsou určeny pro zákazníky České pošty, kteří s Českou poštou uzavřeli smlouvu o poskytování certifikačních služeb. Zákazník (prostřednictvím pověřené osoby) definuje, pro které osoby mají být certifikáty vydány. Osoby, které žádají o certifikáty vydané podle této politiky a užívají je, budou nazývány žadatelé o certifikát. Držitelem certifikátu je zákazník České pošty.

Zákazník odpovídá za vazbu mezi údaji o sobě a údaji, které jsou uvedeny v certifikátu vydaném podle této certifikační politiky. Poskytovatel certifikačních služeb ověřuje vazbu mezi zákazníkem a veřejným klíčem v certifikátu.

Certifikáty vydané podle této certifikační politiky mohou být použity k ověření elektronických podpisů, autentizaci a šifrování dat.

Zákazník uzavře s Českou poštou písemnou smlouvu o poskytování certifikačních služeb tak, jak je v obchodním styku obvyklé. Smlouva se zákazníkem obsahuje seznam pověřených osob, které určují, kterým žadatelům o certifikát mají být vydány certifikáty podle této certifikační politiky. Pověřená osoba doručí České poště seznam žadatelů o certifikát, pro které mají být vydány certifikáty podle této certifikační politiky. Žadatel o certifikát se osobně dostaví na pracoviště registrační autority PostSignum Public CA, kde předloží jeden osobní doklad a elektronickou žádost o certifikát. Pokud je žadatel o certifikát uveden v seznamu žadatelů dodaném pověřenou osobou a pokud je jeho osobní doklad v pořádku, je mu vydán certifikát s veřejným klíčem z elektronické žádosti a s údaji, které odpovídají údajům uvedeným v seznamu žadatelů. Žadatel o certifikát zkontroluje údaje uvedené v certifikátu, a pokud s nimi souhlasí, potvrdí převzetí certifikátu. Tímto okamžikem se zákazník České pošty stává držitelem certifikátu.

Certifikační politika PostSignum Public CA pro komerční serverové certifikáty verze 1.1

Žadatel může požádat o vydání následného certifikátu prostřednictvím elektronicky podepsané zásilky zaslané České poště způsobem, který Česká pošta stanoví. Musí být splněny tyto podmínky:

- zákazník má s Českou poštou uzavřenou platnou smlouvu o poskytování certifikačních služeb,
- zákazník požaduje změnu jen těch údajů v certifikátu, které tato certifikační politika povoluje změnit v následných certifikátech,
- certifikát byl vydán podle některé z těchto certifikačních politik:
 - certifikační politiky PostSignum Public CA pro certifikáty technologických komponent organizací verze 1.50 a vyšší, nebo
 - certifikační politiky PostSignum Public CA pro certifikáty technologických komponent nepodnikajících fyzických osob verze 1.20 a vyšší, nebo
 - certifikační politika PostSignum Public CA pro komerční serverové certifikáty verze 1.0 a vyšší.

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

1.2 Název a jednoznačné určení dokumentu

Tab. 1 Identifikace politiky

Název dokumentu	Certifikační politika PostSignum Public CA pro komerční serverové certifikáty
Verze dokumentu	2.0
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	2.23.134.1.2.1.8.110
Datum vydání	30.1.2010
Doba platnosti	Do odvolání nebo do dne ukončení služeb autorit PostSignum VCA.

1.3 Participující subjekty

Česká pošta, s. p., jako poskytovatel certifikačních služeb, ustavila hierarchii certifikačních autorit s názvem PostSignum, v jejímž rámci je provozována kořenová certifikační autorita PostSignum Root QCA a podřízené certifikační autority poskytující různé certifikační služby. Podřízené certifikační autority mohou být řízeny a provozovány pouze Českou poštou, s.p. (s výjimkou registračních autorit - viz dále).

Identifikační a kontaktní údaje poskytovatele certifikačních služeb jsou:

**Certifikační politika PostSignum Public CA
pro komerční serverové certifikáty verze 1.1**

Česká pošta, s. p.

IČ 47114983, DIČ CZ47114983

Politických vězňů 909/4, 225 99 Praha 1

tel.: 267 196 111

e-mail: info@cpost.cz

1.3.1 Certifikační autority (dále „CA“)

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

PostSignum Public CA vydává komerční certifikáty koncovým uživatelům v souladu s definovanými certifikačními politikami.

1.3.2 Registrační autority (dále „RA“)

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

Registrační autority zajišťují zejména tyto služby:

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

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

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

1.3.2.1 Stacionární registrační autority

Stacionární registrační autority jsou provozovány poskytovatelem certifikačních služeb na obchodních místech a kontaktních místech Veřejné správy České pošty nebo externím subjektem v definované lokalitě.

1.3.2.2 Mobilní registrační autority

Mobilní registrační autority jsou mobilními pracovišti provozovanými Českou poštou nebo externím subjektem.

1.3.2.3 Pracoviště pro příjem žádostí o vydání následného certifikátu

Elektronické žádosti o vydání následného certifikátu (výměna dat pro ověřování elektronických podpisů nebo značek) jsou přijímány na adrese

**Certifikační politika PostSignum Public CA
pro komerční serverové certifikáty verze 1.1**

E-mail: podatelna.postsignum@cpost.cz

1.3.2.4 Nonstop zneplatňující služba

Služba je provozována nepřetržitě 24 hodin denně, je určena výhradně pro příjem žádostí o zneplatnění certifikátu především mimo pracovní dobu registračních autorit České pošty. Kontaktní údaje jsou

Telefon: 556 316 298

Fax: 556 300 013

E-mail: postsignum@cpost.cz

Web: www2.postsignum.cz

1.3.3 Držitelé komerčních certifikátů, kteří požádali o vydání komerčního certifikátu (dále certifikátu), a kterým byl certifikát vydán

1.3.3.1 Zákazníci

Zákazníkem PostSignum VCA je nepodnikající fyzická osoba, podnikající fyzická osoba, právnická osoba, státní orgán nebo orgán místní samosprávy. Zákazník uzavírá písemnou smlouvu o poskytování certifikačních služeb s Českou poštou.

Zákazník České pošty se okamžikem vydání certifikátu žadateli stává držitelem certifikátu.

1.3.3.2 Pověřená osoba

Pověřenou osobou je osoba definovaná zákazníkem při uzavírání smlouvy o poskytování certifikačních služeb. Tato osoba vystupuje vůči poskytovateli certifikačních služeb jako zástupce zákazníka. Určuje zejména, kteří zaměstnanci zákazníka mají právo žádat o certifikát u PostSignum VCA a o jaký certifikát mají právo žádat (včetně typu certifikátu – politiky, podle které bude certifikát vydán).

Česká pošta získá při uzavírání smlouvy seznam pověřených osob zákazníka.

V případě nepodnikajících fyzických osob (občanů) a podnikajících fyzických osob (podnikatelů) se pověřenou osobou automaticky stává samotný zákazník.

1.3.3.3 Žadatel

Žadatel o certifikát je v případě certifikátu vydaného podle této certifikační politiky osoba, která má právo žádat o certifikát. Jedná se o osobu, která je v určitém vztahu se zákazníkem nebo je přímo tímto zákazníkem.

1.3.4 Spoléhající se strany

Spoléhající se stranou (uživatel certifikátu) je libovolný subjekt spoléhající se na certifikát vydaný PostSignum VCA. Spoléhající se strany nevstupují do smluvního vztahu s poskytovatelem certifikačních služeb.

1.3.5 Jiné participující subjekty

1.3.5.1 Externí participující subjekty

Na provozu certifikační autority se dále zejména podílí následující subjekty:

**Certifikační politika PostSignum Public CA
pro komerční serverové certifikáty verze 1.1**

TTC Telekomunikace, s.r.o.

IČ 41194403

Třebohostická 987/5, 100 00 Praha 10

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

Uvedený subjekt zajišťuje provoz a správu externí publikační služby.

ICZ, a.s.

IČ 25145444

Na Hřebenech II 1718/10, 140 00 Praha 4

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

Uvedený subjekt je hlavním dodavatelem certifikační autority PostSignum VCA.

1.3.5.2 Interní participující subjekty

Komise pro certifikační politiky ČP

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

Komise pro certifikační politiky ČP

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

Komisi pro certifikační politiky ČP je možné kontaktovat na adrese

paa.postsignum@cpost.cz

Tým pro tvorbu certifikačních politik ČP

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

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

Komerční certifikáty vydané podle této certifikační politiky mohou být použity pro ověření elektronických podpisů, autentizaci a šifrování dat

1.4.2 Omezení použití certifikátu

Komerční certifikáty vydávané podle této certifikační politiky nejsou primárně určeny 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.

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

1.5 Správa politiky

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

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

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

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

1.5.1 Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

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

1.5.2 Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

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

manager.postsignum@cpost.cz

nebo na webových stránkách poskytovatele

<http://vca.postsignum.cz>

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

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

1.5.4 Postupy při schvalování souladu podle 1.5.3

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

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

- při 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.

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

1.6 Přehled použitých pojmů a zkratk

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

Držitel certifikátu – zákazník od okamžiku vydání certifikátu.

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

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

Kvalifikovaný certifikát – kvalifikovaný certifikát ve smyslu [ZoEP].

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

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

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

PostSignum – hierarchie certifikačních autorit tvořená kořenovou certifikační autoritou PostSignum Root QCA a všemi podřízenými certifikačními autoritami, pro něž PostSignum Root QCA vydala certifikát.

Certifikační politika PostSignum Public CA pro komerční serverové certifikáty verze 1.1

PostSignum VCA – hierarchie certifikačních autorit, vydávajících komerční certifikáty a komerční systémové certifikáty.

PostSignum Root QCA – kořenová certifikační autorita, která má samopodepsaný kvalifikovaný systémový certifikát. Vydává komerční 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 komerční certifikáty a komerční systémové certifikáty pro subjekty, které nejsou certifikačními autoritami.

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

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

VCA ČP – viz PostSignum VCA.

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

Rozlišovací jméno – jednoznačně identifikuje držitele certifikátu dle pravidel definovaných příslušnou certifikační politikou.

Soukromý klíč – souhrnné označení dat pro vytváření elektronického podpisu, šifrování nebo autentizaci.

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 elektronického podpisu či značky nebo pro zajištění jiných bezpečnostních služeb. Jinak též označována jako Osoba spoléhající se na certifikát.

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

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

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

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

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

**Certifikační politika PostSignum Public CA
pro komerční serverové certifikáty verze 1.1**

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

Žadatel – osoba, která má právo žádat u PostSignum Public CA o certifikát podle některé z platných certifikačních politik.

2 ODPOVĚDNOST ZA ZVEŘEJŇOVÁNÍ A ÚLOŽIŠTĚ INFORMACÍ A DOKUMENTACE

2.1 Úložiště informací a dokumentace

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

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

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

2.2 Zveřejňování informací a dokumentace

Vydané certifikáty jsou uloženy v databázi certifikační autority.

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

2.2.1 Zveřejňování certifikátů a CRL

Certifikáty certifikačních autorit jsou zveřejňovány

- na webových stránkách PostSignum VCA
 - <http://www.postsignum.cz>,
 - <http://www2.postsignum.cz>,
 - <http://postsignum.ttc.cz>, nebo
- na obchodních místech České pošty, kde je možné požádat o jejich zkopírování na přinesené médium.

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

- na webových stránkách PostSignum VCA
 - <http://www.postsignum.cz>.
 - <http://www2.postsignum.cz>

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

- na webových stránkách PostSignum VCA
 - <http://www.postsignum.cz>
 - <http://www2.postsignum.cz>
 - <http://postsignum.ttc.cz>

2.2.2 Zveřejňování informací o certifikační autoritě

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

**Certifikační politika PostSignum Public CA
pro komerční serverové certifikáty verze 1.1**

- webových stránkách PostSignum VCA
<http://www.postsignum.cz>, nebo

- obchodních místech pouze k nahlédnutí.

Další důležité informace (např. zneplatnění systémového certifikátu certifikační autority) nebo informace o mimořádné události jsou zveřejňovány

- na webových stránkách PostSignum VCA
<http://www.postsignum.cz>
- na obchodních místech a registračních autoritách ve formě vyvěšeného textového oznámení,
- v celostátně distribuovaném deníku (konkrétně deníku Hospodářské noviny).

2.3 Periodicita zveřejňování informací

Informace jsou zveřejňovány v následujících intervalech:

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

2.4 Řízení přístupu k jednotlivým typům úložišť

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

Poskytovatel certifikačních služeb neumožňuje 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 kritéria.

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

3 IDENTIFIKACE A AUTENTIZACE

3.1 Pojmenování

3.1.1 Typy jmen

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

E-mailová adresa uvedená v rozšíření Subject Alternative Name certifikátu odpovídá standardu RFC-822.

3.1.2 Požadavek na významovost jmen

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

3.1.3 Anonymita a používání pseudonymu

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

3.1.4 Pravidla pro interpretaci různých forem jmen

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

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

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

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

3.1.5 Jedinečnost jmen

Každý zákazník v systému certifikační autority má přiřazen jedinečný identifikátor, který je uložen v údaji „serialNumber“ v Subjectu certifikátu. Zákazník je dále zodpovědný za zaručení jednoznačnosti rozlišovacího jména v subjectu certifikátu vydaného podle této certifikační politiky v rámci zákazníka.

V položce Subject certifikátu je uvedena kombinace jednoznačných údajů o zákazníkovi (IČ zákazníka a jméno zákazníka) a jednoznačného rozlišovacího jména, čímž je zaručeno, že dvěma různým žadatelům nebudou vydány certifikáty se stejnou položkou Subject.

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 pověřeným osobám zákazníků (resp. zákazníkům) do dvou pracovních dnů od vzniku kolize.

3.1.6 Obchodní značky

Všechna pole certifikátu, která PostSignum VCA ověřuje, mají předepsanou strukturu a musí být doložena jejich správnost a úplnost (viz ustanovení odstavce 3.2.3).

Certifikační politika PostSignum Public CA pro komerční serverové certifikáty verze 1.1

Odpovědnost za použití obchodních značek nebo registrovaných ochranných známek v polích certifikátu, které nejsou PostSignum VCA ověřovány (viz odstavec 3.2.4), má zákazník.

3.2 Počáteční ověření identity

3.2.1 Ověřování souladu dat, tj. postup při ověřování, zda má osoba soukromý klíč odpovídající veřejnému klíči

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

3.2.2 Ověřování identity právnické osoby nebo organizační složky státu

Následující ustanovení jsou platná rovněž pro podnikající fyzické osoby s přiděleným identifikačním číslem, vystupující v roli zákazníka.

3.2.2.1 Uzavření smlouvy se zákazníkem

Zákazník uzavírající smlouvu o poskytování certifikačních služeb prokazuje svou totožnost tak, jak je v obchodním styku obvyklé. Zákazník odpovídajícím způsobem prokazuje oprávněnost použití názvu organizace, který bude uveden v certifikátech.

Smlouva o poskytování certifikačních služeb obsahuje mj. seznam pověřených osob, které budou s poskytovatelem certifikačních služeb komunikovat ohledně vydávání certifikátů. Smlouva je uzavřena tak, jak je v obchodním styku obvyklé (statutární zástupce organizace apod.).

3.2.2.2 Změna pověřené osoby

V době platnosti smlouvy může dojít ke změně ve jmenování pověřených osob. Změna musí být zachycena v dodatku smlouvy, kde bude uvedena nová pověřená osoba.

3.2.2.3 Pre-Registrace žádosti o certifikát

Pověřená osoba stvrzuje svým podpisem správnost seznamů žadatelů o certifikát. Pracovník registrační autority ověřuje totožnost pověřené osoby a kontroluje, zda se pověřená osoba nachází na aktuálním seznamu pověřených osob.

3.2.3 Ověřování identity fyzické osoby

3.2.3.1 Ověřování identity podnikající fyzické osoby nebo zaměstnance organizace

Podnikající fyzická osoba prokazuje svou totožnost při pre-registraci údajů zákazníka a při podávání žádosti o vydání a zneplatnění certifikátu. Zaměstnanec organizace prokazuje svou totožnost při podávání žádosti o vydání a zneplatnění certifikátu. Předkládá jeden platný, nepoškozený osobní doklad.

Předložený osobní doklad z níže uvedeného seznamu je akceptován za předpokladu, že z něj lze zjistit údaje o státním občanství, o totožnosti, fotografii držitele, rodné číslo (resp. datum narození u cizinců) a údaj o době platnosti dokladu.

- Občané České republiky předkládají občanský průkaz nebo cestovní pas.
- Cizinci předkládají cestovní, diplomatický, služební nebo jinak nazývaný pas vydaný cizím státem nebo samostatný průkaz o povolení k pobytu vydávaný orgány ČR.

**Certifikační politika PostSignum Public CA
pro komerční serverové certifikáty verze 1.1**

Občané členských států Evropské unie a dále občané Islandu, Lichtenštejnska, Norska a Švýcarska mohou předložit také osobní doklad, který jim byl vydán k prokazování totožnosti na území příslušného státu.

Pracovník registrační autority zkontroluje:

- zda je doklad platný,
- zda fotografie na dokladu odpovídá žadateli o certifikát.

3.2.3.2 Ověřování identity nepodnikající fyzické osoby

Nepodnikající fyzická osoba prokazuje svou totožnost při uzavírání smlouvy o poskytování certifikačních služeb a při podávání žádosti o certifikát. Předkládá jeden platný, nepoškozený osobní doklad a jeden platný, nepoškozený doplňující osobní doklad.

Předložený osobní doklad z níže uvedeného seznamu je akceptován za předpokladu, že z něj lze zjistit údaje o státním občanství, o totožnosti, fotografii držitele, rodné číslo (resp. datum narození u cizinců) a údaj o době platnosti dokladu.

- Občané České republiky předkládají jako osobní doklad platný občanský průkaz nebo cestovní pas.
- Cizinci předkládají jako osobní doklad cestovní, diplomatický, služební nebo jinak nazývaný pas vydaný cizím státem, cizinecký pas s územní platností do všech států světa, cestovní průkaz totožnosti nebo samostatný průkaz o povolení k pobytu vydávaný orgány ČR.
Občané členských států Evropské unie a dále občané Islandu, Lichtenštejnska, Norska a Švýcarska mohou předložit jako osobní doklad také osobní doklad, který jim byl vydán k prokazování totožnosti na území příslušného státu.

Předložený doplňující osobní doklad z níže uvedeného seznamu je akceptován za předpokladu, že nebyl použit jako osobní doklad.

- Občané České republiky předkládají jako doplňující osobní doklad občanský průkaz, cestovní pas, řidičský průkaz, průkaz ZTP nebo rodný list.
- Cizinci předkládají jako doplňující osobní doklad cestovní, diplomatický, služební nebo jinak nazývaný pas vydaný cizím státem, cizinecký pas s územní platností do všech států světa, cestovní průkaz totožnosti, samostatný průkaz o povolení k pobytu vydávaný orgány ČR nebo řidičský průkaz Evropské unie.
Cizinci mohou předložit jako doplňující osobní doklad také osobní doklad, který jim byl vydán k prokazování totožnosti na území příslušného státu. Typ dokladu a údaje na dokladu musí být psány latinkou a doklad musí obsahovat anglický překlad uvedených údajů.

Pracovník registrační autority zkontroluje:

- zda jsou doklady platné,
- zda fotografie na dokladech odpovídá žadateli o certifikát.

3.2.4 Neověřené informace vztahující se k držiteli certifikátu

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

Certifikační politika PostSignum Public CA pro komerční serverové certifikáty verze 1.1

Česká pošta, jakožto poskytovatel certifikačních služeb, dále neověřuje správnost údaje organizační jednotka, uvedeného v seznamu žadatelů, který předává poskytovateli certifikačních služeb pověřená osoba zákazníka.

3.2.5 Ověřování specifických práv

Žádná ustanovení v tomto odstavci.

3.2.6 Kritéria pro interoperabilitu

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

3.3 Identifikace a autentizace při zpracování požadavků na výměnu veřejného klíče v certifikátu

3.3.1 Identifikace a autentizace při rutinní výměně soukromého klíče a jemu odpovídajícího veřejného klíče (dále „párová data“)

Identita žadatele o vydání následného certifikátu je ověřena při ověřování elektronického podpisu na žádosti o vydání následného certifikátu. Pro podpis příslušné žádosti musí být použit platný certifikát (certifikát nebyl zneplatněn a ani neskončila jeho platnost) náležející žadateli a vydaný podle:

- certifikační politiky PostSignum Public CA pro certifikáty zaměstnanců nebo podnikajících fyzické osoby verze 1.50 a vyšší, nebo
- certifikační politiky PostSignum Public CA pro certifikáty fyzických osob verze 1.20 a vyšší, nebo
- certifikační politiky PostSignum Public CA pro komerční osobní certifikáty verze 1.0 a vyšší.
- certifikační politiky PostSignum Qualified CA pro certifikáty určené k ověření elektronického podpisu zaměstnance verze 1.21 a vyšší, nebo
- certifikační politiky PostSignum Qualified CA pro certifikáty určené k ověření elektronického podpisu fyzické osoby verze 1.21 a vyšší, nebo
- certifikační politiky PostSignum Qualified CA pro kvalifikované osobní certifikáty verze 1.0 a vyšší.

3.3.2 Identifikace a autentizace při výměně párových dat po zneplatnění certifikátu

V případě zneplatnění certifikátu je nutné při identifikaci a autentizaci spojené s vydáním nového certifikátu postupovat stejně jako v případě počátečního ověření identity při vydání prvního certifikátu (viz odst. 3.2.3).

3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu

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

- znalostí hesla pro zneplatnění, které zadal při registraci žádosti o certifikát, nebo
- jedním osobním dokladem v případě zaměstnance organizace či podnikající fyzické osoby, nebo jedním osobním dokladem a jedním doplňujícím dokladem v případě nepodnikající fyzické osoby (viz odst. 3.2.3).

**Certifikační politika PostSignum Public CA
pro komerční serverové certifikáty verze 1.1**

Pověřená osoba prokáže svou totožnost:

- podpisem písemné žádosti o zneplatnění certifikátu, nebo
- elektronickým podpisem, založeným na certifikátu vydaném podřízenou certifikační autoritou z hierarchie PostSignum, na elektronicky zaslané žádosti o zneplatnění certifikátu, nebo
- osobním dokladem při podání žádosti o zneplatnění certifikátu osobně na registrační autoritě České pošty; pracovník registrační autority dále ověřuje, zda se pověřená osoba nachází na aktuálním seznamu pověřených osob.

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

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

4.1 Žádost o vydání certifikátu

4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu

Žádost o vydání certifikátu podle této certifikační politiky mohou podat:

- osoby určené pověřenou osobou zákazníka – organizace, nebo
- podnikající fyzické osoby, které uzavřely smlouvu o poskytování certifikačních služeb, nebo
- nepodnikající fyzické osoby, které uzavřely smlouvu o poskytování certifikačních služeb.

4.1.2 Registrační proces a odpovědnosti poskytovatele a žadatele

4.1.2.1 Uzavření smlouvy

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

Zákazník předá České poště vyplněný formulář smlouvy, který je k dispozici na webové stránce poskytovatele, a zástupce ČP svým podpisem uzavře se zákazníkem smlouvu o poskytování certifikačních služeb.

Formuláře smlouvy obsahují odkazy na webové stránky, na nichž je možno získat Certifikační politiky a aktuální ceník.

Certifikační politika a aktuální ceník se stávají součástí smlouvy o poskytování služeb spolu s [VOP] ke dni uzavření smlouvy o poskytování služeb.

Smlouva o poskytování certifikačních služeb obsahuje mimo jiné:

- identifikační údaje zákazníka (je-li to relevantní, včetně IČ a případně rozšířeného IČ),
- rozsah poskytovaných certifikačních služeb,
- seznam pověřených osob, které budou s poskytovatelem certifikačních služeb komunikovat ohledně vydávání certifikátů.

Smlouva je se zákazníkem uzavřena tak, jak je v obchodním styku obvyklé (statutární zástupce organizace apod.). Smlouva musí být uzavřena v písemné formě.

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

4.1.2.2 Pre-registrace žadatelů o certifikát

Pre-registrací se rozumí postup, kdy pověřená osoba v případě zákazníka – organizace schvaluje seznam žadatelů, kteří mohou žádat o certifikát podle této certifikační politiky, a tento seznam předává poskytovateli certifikačních služeb. V případě podnikající a nepodnikající fyzické osoby předává samotný zákazník údaje o jediném žadateli.

Seznam žadatelů obsahuje povinné a nepovinné údaje certifikátu, jež jsou uvedeny v odst. 7.1. Rodné číslo resp. datum narození žadatele není ve vydaném certifikátu uvedeno.

Dále pověřená osoba nebo samotný zákazník určuje, zda-li může být vydaný certifikát zveřejněn široké veřejnosti bez omezení.

Certifikační politika PostSignum Public CA pro komerční serverové certifikáty verze 1.1

Česká pošta si vyhrazuje právo odmítnout pre-registraci, vyskytnou-li se jakékoliv pochybnosti o obsahu položky Subject certifikátu.

Registrační autorita PostSignum Public CA ověřuje totožnost žadatele o certifikát pomocí dokladů uvedených v kapitole 3.2. Vazbu mezi žadatelem a zákazníkem (organizací) uvedeným v certifikátu garantuje pověřená osoba zákazníka (organizace), která spravuje seznam žadatelů předávaný poskytovateli certifikačních služeb.

4.1.2.3 Odpovědnost 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 pověřených 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.

Je-li zákazníkem podnikající nebo nepodnikající fyzická osoba, vztahují se na něj též odpovědnosti žadatele uvedené v odst. 4.1.2.5.

4.1.2.4 Odpovědnost pověřených osob

Pověřená 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 údaj CN zvolený pro certifikát je v rámci zákazníka jednoznačný,
- doložit čestné prohlášení o vlastnictví domény, v případě, že zvolené CN má tvar doménového jména.

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

Pověřená osoba nebo samotný zákazník České poště sděluje, ve kterých certifikátech má být uvedený Identifikátor klienta přidělovaný Ministerstvem práce a sociálních věcí.

4.1.2.5 Odpovědnost žadatele

Žadatel je povinen zejména:

- poskytovat pravdivé a úplné informace při pre-registraci žádosti o certifikát a při registraci žádosti o vydání následného certifikátu,
- zkontrolovat, zda údaje uvedené v certifikátu jsou správné a odpovídají požadovaným údajům,

Certifikační politika PostSignum Public CA
pro komerční serverové certifikáty verze 1.1

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

4.1.2.6 Odpovědnost poskytovatele

Poskytovatel certifikačních služeb je zejména povinen:

- v procesu registrace zákazníka a žadatele o certifikát ověřit všechny údaje podle předložených dokladů,
- do dvou pracovních dnů od podání žádosti posoudit žádost o certifikát resp. žádost o následný certifikát, vydat rozhodnutí, zda bude certifikát vydán, a o tomto rozhodnutí informovat žadatele nebo zákazníka,
- vydat certifikát obsahující věcně správné údaje na základě informací, které jsou certifikační autoritě k dispozici v době vydávání certifikátu,
- zveřejňovat certifikační politiky, podle kterých vydává certifikáty, na webových stránkách PostSignum VCA, případně jinými vhodnými způsoby (viz. odstavec 2.2),
- zveřejnit kvalifikovaný systémový certifikát poskytovatele certifikačních služeb tak, aby se každý mohl ujistit o jeho identitě,
- věnovat náležitou péči všem činnostem spojeným s poskytováním certifikačních služeb; náležitá péče zahrnuje provoz v souladu
 - s platnými právními předpisy,
 - s touto certifikační politikou,
 - s certifikační prováděcí směrnicí,
 - se systémovou bezpečnostní politikou,
 - s provozní dokumentací.

4.2 Zpracování žádosti o certifikát

4.2.1 Identifikace a autentizace

Žadatel o certifikát se dostaví na pracoviště registrační autority, kde předloží:

- jeden osobní doklad v případě zaměstnance organizace nebo podnikající fyzické osoby, resp.
- jeden osobní doklad a jeden doplňující osobní doklad v případě nepodnikající fyzické osoby.

Certifikační politika PostSignum Public CA pro komerční serverové certifikáty verze 1.1

Dále žadatel poskytne pracovníkovi registrační autority elektronickou žádost ve formátu PKCS#10 obsahující veřejný klíč, a to buď na médiu nebo jiným způsobem upřesněným na webových stránkách PostSignum VCA.

Žadatel o certifikát při registraci zadává rovněž heslo, pomocí kterého bude certifikát v případě potřeby zneplatňovat.

Pracovník registrační autority zkontroluje osobní doklad žadatele o certifikát. Oproti seznamu žadatelů ověří, zda daná osoba skutečně smí žádat o certifikát dle dané certifikační politiky a zda údaje v elektronické žádosti souhlasí s údaji v seznamu žadatelů.

4.2.2 Přijetí nebo zamítnutí žádosti o certifikát

Pokud údaje v elektronické žádosti předložené žadatelem 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.

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 žadatele o certifikát.

4.2.3 Doba zpracování žádosti o certifikát

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 kladného rozhodnutí je poskytovatel povinen vydat certifikát do následujícího pracovního dne.

4.3 Vydání certifikátu

Po kontrole 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.

4.3.1 Úkony CA v průběhu vydávání certifikátu

Certifikát je vydán systémem certifikační autority automaticky po přijetí žádosti schválené pracovníkem registrační autority.

4.3.2 Oznámení o vydání certifikátu držiteli certifikátu

Pracovník registrační autority předává žadateli výtisk protokolu o vydání certifikátu s údaji uvedenými v certifikátu bezprostředně po vydání certifikátu nebo je na emailovou adresu žadatele odeslána informace o umístění vydaného certifikátu (URL), kde je možné vydaný certifikát akceptovat (potvrdit převzetí certifikátu) a stáhnout.

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

Poté, co je certifikát vydán, žadatel o certifikát zkontroluje správnost údajů uvedených v certifikátu a potvrdí převzetí certifikátu.

Certifikační politika PostSignum Public CA pro komerční serverové certifikáty verze 1.1

Převzetím 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 může dojít k neoprávněnému použití soukromého klíče odpovídajícího veřejnému klíči v certifikátu,
- že údaje ve vydaném certifikátu jsou správné a úplné (zejména, že veřejný klíč v certifikátu odpovídá veřejnému klíči uvedenému v poskytnuté PKCS#10 žádosti).

Převzetím certifikátu žadatelem se zákazník stává držitelem certifikátu.

Vydaný certifikát je žadateli předán ve formátu DER.

4.4.2 Zveřejňování vydaných certifikátů poskytovatelem

Certifikáty vydané PostSignum Public CA, u nichž byl vysloven souhlas se zveřejněním, jsou zveřejňovány elektronickou cestou nejpozději do 24 hodin od převzetí certifikátu žadatelem.

4.4.3 Oznámení o vydání certifikátu jiným subjektům

Kromě zveřejnění vydaného certifikátu, u kterého byl držitelem vysloven souhlas se zveřejněním, a zaslání oznámení žadateli a volitelně pověřené osobě zákazníka neoznamuje poskytovatel certifikačních služeb vydání certifikátu žádné třetí straně.

4.5 Použití párových dat a certifikátů

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

4.5.1 Použití soukromého klíče a certifikátu držitelem certifikátu

Držitel certifikátu:

- nakládá se soukromým klíčem, který odpovídá veřejnému klíči v certifikátu vydaném podle této certifikační politiky, s náležitou péčí, a to tak, aby nemohlo dojít k jeho neoprávněnému použití,
- v případě ztráty, odcizení nebo podezření na kompromitaci soukromého klíče neprodleně informuje poskytovatele certifikačních služeb a zároveň ukončí používání uvedeného soukromého klíče,
- užívá soukromý klíč a odpovídající certifikát vydaný podle této certifikační politiky pouze pro účely stanovené v této certifikační politice, uvedené v odst. 1.4.1, tj. pro vytváření elektronického podpisu, k autentizaci a šifrování.

4.5.2 Použití veřejného klíče a certifikátu spoléhající se stranou

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

- získá certifikáty PostSignum Public CA a PostSignum Root QCA z bezpečného zdroje (webové stránky PostSignum VCA, webové stránky ministerstva podle [V378], na obchodním místě) a ověří otisk ("fingerprint") těchto certifikátů.
- před použitím certifikátu vydaného PostSignum Public CA ověří platnost certifikátu PostSignum Public CA a následně i platnost vydaného koncového certifikátu; kontrola se

Certifikační politika PostSignum Public CA pro komerční serverové certifikáty verze 1.1

provádí na správnost podpisu vydávající autority a vůči příslušnému aktuálnímu CRL a aktuálnímu času (tuto činnost obvykle vykonává aplikace uživatele certifikátu).

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

4.6 Obnovení certifikátu

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

4.6.1 Podmínky pro obnovení certifikátu

PostSignum VCA tuto službu neposkytuje.

4.6.2 Subjekty oprávněné požadovat obnovení certifikátu

PostSignum VCA tuto službu neposkytuje.

4.6.3 Zpracování požadavku na obnovení certifikátu

PostSignum VCA tuto službu neposkytuje.

4.6.4 Oznámení o vydání obnoveného certifikátu držiteli certifikátu

PostSignum VCA tuto službu neposkytuje.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu

PostSignum VCA tuto službu neposkytuje.

4.6.6 Zveřejňování vydaných obnovených certifikátů poskytovatelem

PostSignum VCA tuto službu neposkytuje.

4.6.7 Oznámení o vydání obnoveného certifikátu jiným subjektům

PostSignum VCA tuto službu neposkytuje.

4.7 Výměna veřejného klíče v certifikátu

Služba výměny veřejného klíče v certifikátu je označována jako vydání následného certifikátu. Toto označení bude dále používáno i dále v textu.

4.7.1 Podmínky pro výměnu veřejného klíče v certifikátu

Vydání následného certifikátu podle této certifikační politiky je možné pouze za předpokladu, že

- zákazník má s Českou poštou uzavřenou platnou smlouvu o poskytování certifikačních služeb,
- certifikát, o jehož následný certifikát je žádáno, nebyl zneplatněn,
- zákazník požaduje změnu jen těch údajů v certifikátu, které tato certifikační politika umožňuje změnit v následných certifikátech,
- certifikát, o jehož následný certifikát je žádáno, byl vydán podle některé z těchto certifikačních politik:

Certifikační politika PostSignum Public CA pro komerční serverové certifikáty verze 1.1

- certifikační politiky PostSignum Public CA pro certifikáty technologických komponent organizací verze 1.50 a vyšší, nebo
 - certifikační politiky PostSignum Public CA pro certifikáty technologických komponent nepodnikajících fyzických osob verze 1.20 a vyšší, nebo
 - certifikační politika PostSignum Public CA pro komerční serverové certifikáty verze 1.0 a vyšší.
- žadatel žádající o vydání následného certifikátu vlastní certifikát vydaný podle některé z těchto certifikačních politik (certifikát je použit pro ověření podpisu na zásilce žádající o obnovu certifikátu):
- certifikační politika PostSignum Qualified CA pro certifikáty určené k ověření elektronického podpisu zaměstnance verze 1.21 a vyšší, nebo
 - certifikační politika PostSignum Qualified CA pro certifikáty určené k ověření elektronického podpisu fyzické osoby verze 1.21 a vyšší, nebo
 - certifikační politika PostSignum Qualified CA pro kvalifikované osobní certifikáty verze 1.0 a vyšší.
 - certifikační politika PostSignum Public CA pro certifikáty zaměstnanců nebo podnikající fyzické osoby verze 1.50 a vyšší, nebo
 - certifikační politika PostSignum Public CA pro certifikáty fyzických osob verze 1.20 a vyšší, nebo
 - certifikační politika PostSignum Public CA pro komerční osobní certifikáty verze 1.0 a vyšší.

Pokud nejsou splněny všechny tyto podmínky, není vydání následného certifikátu možné, a je nutné použít postup popsany v odst. 4.2.

4.7.2 Subjekty oprávněně požadovat výměnu veřejného klíče v certifikátu

Žádost o vydání následného certifikátu podle této certifikační politiky mohou podat osoby určené pověřenou osobou zákazníka nebo samotný zákazník, viz odst. 4.1.2.2.

4.7.3 Zpracování požadavku na výměnu veřejného klíče

Žadatel o následný certifikát zašle žádost o vydání následného certifikátu na vyhrazené pracoviště registrační autority (viz kapitola 1.3.2.3). Zasílá se zásilka podepsaná elektronickým podpisem založeným na komerčním certifikátu žadatele vydaném PostSignum Public CA nebo podepsaná zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu žadatele vydaném PostSignum Qualified CA. Způsob zaslání elektronické zásilky stanovuje poskytovatel certifikačních služeb na webových stránkách PostSignum VCA.

Žádost o vydání následného certifikátu obsahuje následující informace:

- sériové číslo certifikátu, o jehož následný certifikát je žádáno,
- typ certifikátu (označení certifikační politiky), o jehož následný certifikát je žádáno, a vydávající certifikační autoritu,
- návrh na heslo pro zneplatnění (heslo musí obsahovat min. 8 znaků, z toho min. jedno malé písmeno, min. jedno velké písmeno, min. jednu číslici a min. jeden neabecední znak).

Certifikační politika PostSignum Public CA pro komerční serverové certifikáty verze 1.1

Dále musí zásilka obsahovat elektronickou žádost ve formátu PKCS#10 obsahující veřejný klíč, která je podepsána soukromým klíčem odpovídajícím veřejnému klíči uvedenému v žádosti.

Pracovník registrační autority ověří elektronický podpis na zásilce, zejména platnost certifikátu použitého pro ověření podpisu v době doručení zásilky na Českou poštu (musí být platný), jeho vydávající certifikační autoritu (PostSignum Public CA nebo PostSignum Qualified CA) a zkontroluje ostatní náležitosti zásilky.

Pokud se nepodaří ověřit elektronický podpis na žádosti o vydání následného certifikátu nebo nebudou splněny všechny podmínky pro vydání následného certifikátu, odmítne pracovník registrační autority certifikát vydat a o tomto informuje žadatele.

Česká pošta si vyhrazuje právo odmítnout vydat následný certifikát žadateli podle této certifikační politiky.

Poskytovatel certifikačních služeb je povinen do dvou pracovních dnů od doručení zásilky se žádostí o vydání následného certifikátu posoudit žádost o certifikát, vydat rozhodnutí, zda bude následný certifikát vydán, a o tomto rozhodnutí informovat žadatele o certifikát. Od okamžiku kladného rozhodnutí je poskytovatel povinen vydat certifikát do následujícího pracovního dne.

Po zpracování zásilky se žádostí o certifikát vloží operátor registrační autority vlastní elektronickou 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.

V případě, že heslo pro zneplatnění bylo zasláno v nešifrované formě nebo nesplňovalo požadavky na něj kladené, vygeneruje pracovník registrační autority náhodně nové heslo, které bude uvedeno v protokolu o vydání certifikátu.

Následný certifikát bude obsahovat údaje podle aktuálního seznamu žadatelů (včetně povolených změn), a to bez ohledu na obsah elektronické žádosti o certifikát.

Certifikát se stává platným okamžikem vydání.

4.7.4 Oznámení o vydání certifikátu s vyměněným veřejným klíčem

Na emailovou adresu žadatele je odeslána informace o umístění vydaného certifikátu (URL), kde je možné vydaný certifikát akceptovat (potvrdit převzetí certifikátu) a stáhnout.

4.7.5 Úkony spojené s převzetím certifikátu s vyměněným veřejným klíčem

Žadatel přistoupí na stránku nacházející se na zasláném URL, která bude obsahovat

- údaje o vydaném certifikátu,
- certifikační politiku, podle které byl certifikát vydán, a
- volbu akceptovat/neakceptovat vydaný certifikát.

V případě, že žadatel souhlasí s obsahem certifikátu a ustanoveními příslušné certifikační politiky, zvolí volbu Akceptovat. Pokud žadatel s obsahem certifikátu nesouhlasí, má k dispozici volbu Neakceptovat.

Akceptací následného certifikátu žadatel stvrzuje:

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

**Certifikační politika PostSignum Public CA
pro komerční serverové certifikáty verze 1.1**

- že mu nejsou známy žádné skutečnosti, které by svědčily o tom, že může dojít k neoprávněnému použití soukromého klíče odpovídajícího veřejnému klíči v certifikátu,
- že údaje ve vydaném certifikátu jsou správné a úplné.

Zákazník se akceptací následného certifikátu žadatelem stává držitelem certifikátu.

Vydaný certifikát je žadateli nabídnut ke stažení ve formátu PEM a DER. Žadatel má dále možnost stáhnout elektronickou verzi protokolu o vydání certifikátu.

4.7.6 Zveřejňování vydaných certifikátů s vyměněným veřejným klíčem

Pro zveřejňování následného certifikátu platí stejná pravidla jako pro zveřejňování prvotního certifikátu vydaného obvyklým způsobem (viz odst. 4.4.2).

4.7.7 Oznámení o vydání certifikátu s vyměněným veřejným klíčem jiným subjektům

Pro oznámení o vydání následného certifikátu platí stejná pravidla jako pro oznámení o vydání prvotního certifikátu vydaného obvyklým způsobem (viz odst. 4.4.3).

4.8 Změna údajů v certifikátu

Certifikát se změnami údajů lze vydat pouze

- jako nový certifikát podle postupů uvedených v odstavcích 4.1 - 0, nebo
- jako následný certifikát podle postupů uvedených v odst. 4.7, pokud byly změněny pouze údaje, které dovoluje tato certifikační politika změnit v následných certifikátech.

Změna údajů musí být zákazníkem oznámena poskytovateli odpovídajícím způsobem ještě před podáním žádosti o nový nebo následný certifikát.

Pokud pozbývá pravdivosti některý z údajů uvedených v aktuálním certifikátu, je nutné rovněž odpovídajícím způsobem požádat o zneplatnění aktuálního certifikátu.

4.8.1 Podmínky pro změnu údajů v certifikátu

Veškeré změny údajů v certifikátu musí být poskytovateli certifikačních služeb hlášeny změnovým seznamem žadatelů.

4.8.2 Subjekty oprávněné požadovat změnu údajů v certifikátu

Změnový seznam žadatelů podává pověřená osoba zákazníka (organizace), nebo samotný zákazník (podnikající nebo nepodnikající fyzická osoba).

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

Pracovník registrační autority ověří:

- v případě pověřené osoby, zda je tato uvedena na aktuálním seznamu pověřených osob zákazníka, a její identitu prostřednictvím osobního dokladu,
- v případě samotného zákazníka, zda má uzavřenou platnou smlouvu o poskytování certifikačních služeb, a jeho identitu prostřednictvím osobního dokladu.

Pracovník registrační autority poté aktualizuje údaje o žadateli a certifikátu v systému certifikační autority.

4.8.4 Oznámení o vydání certifikátu se změněnými údaji

Totožné s vydáním prvního certifikátu. Viz ustanovení odstavce 4.3.2.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Totožné s převzetím prvního certifikátu. Viz ustanovení odstavce 4.4.1.

4.8.6 Zveřejňování vydaných certifikátů se změněnými údaji

Totožné se zveřejněním prvního certifikátu. Viz ustanovení odstavce 4.4.2.

4.8.7 Oznámení o vydání certifikátu se změněnými údaji jiným subjektům

Totožné s oznámením o vydání prvního certifikátu. Viz ustanovení odstavce 4.4.3.

4.9 Zneplatnění a pozastavení platnosti certifikátu

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

Pokud není certifikát po dobu jeho platnosti nutné zneplatnit, skončí jeho platnost v časovém okamžiku uvedeném v certifikátu. Každý vydaný certifikát zůstává po ukončení své platnosti nadále uložen v databázi vydávající certifikační autority a archivován v souladu s platnou legislativou a archivačními předpisy České pošty.

4.9.1 Podmínky pro zneplatnění certifikátu

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,
- další důvody (úmrtí, zánik, zbavení nebo omezení právní způsobilosti držitele; pozbytí pravdivosti údajů, na jejichž základě byl certifikát vydán).

4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

O zneplatnění certifikátu může požádat:

- zákazník (držitel certifikátu) prostřednictvím pověřené osoby nebo osobně (jedná-li se o podnikající nebo nepodnikající fyzickou osobu),
- žadatel o certifikát,
- manažer certifikační autority, která vydala certifikát, nebo

4.9.3 Požadavek na zneplatnění certifikátu

4.9.3.1 Žádost o zneplatnění certifikátu podaná osobně žadatelem na registrační autoritě

Žadatel požádá o zneplatnění certifikátu osobně na pracovišti registrační autority, kde prokáže svou totožnost stejným způsobem jako při podávání žádosti o certifikát (viz odst. 3.2.3). Podepíše písemnou žádost o zneplatnění certifikátu, kterou vytiskne pracovník registrační autority. Žádost

Certifikační politika PostSignum Public CA pro komerční serverové certifikáty verze 1.1

obsahuje sériové číslo certifikátu, jméno vydávající certifikační autority a volitelně i důvod zneplatnění.

Operátor registrační autority vyhledá certifikát a zahájí proces zneplatnění. Ověří, zda žadatel má 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.

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

Žadatel podává žádost o zneplatnění certifikátu telefonicky nebo faxem na telefonní číslo uvedené 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 musí obsahovat sériové číslo certifikátu, jméno vydávající certifikační autority, heslo pro zneplatnění certifikátu a volitelně důvod zneplatnění. Žádost podaná faxem musí být vlastnoručně podepsána žadatelem.

Operátor oprávněný provádět zneplatnění zkontroluje heslo pro zneplatnění v žádosti oproti heslu zadanému při registraci žádosti o certifikát. V případě, že údaje souhlasí, certifikát je zneplatněn. V opačném případě operátor zneplatnění neprovede a informuje žadatele.

Pokud bylo zneplatnění úspěšné, je vytvořen protokol o zneplatnění, který je prostřednictvím elektronické pošty zaslán pověřené osobě. Žadatel je o zneplatnění certifikátu informován prostřednictvím elektronické pošty na adresu uvedenou ve zneplatněném certifikátu (pokud certifikát adresu elektronické pošty obsahuje).

4.9.3.3 Žádost o zneplatnění certifikátu podaná pověřenou osobou

V případě, že o zneplatnění žádá zákazník, učiní tak písemnou formou. Pověřená osoba se dostaví osobně na registrační autoritu České pošty, kde s ní bude sepsána žádost o zneplatnění certifikátu. Písemnou žádost může pověřená osoba také zaslat faxem na číslo uvedené v odst. **Chyba! Nenalezen zdroj odkazů.**

Pokud pověřená osoba vlastní certifikát určený k podpisu, vydaný podřízenou certifikační autoritou v hierarchii PostSignum, může zaslat žádost o zneplatnění certifikátu v e-mailové zprávě opatřené elektronickým podpisem na adresu uvedenou v odst. **Chyba! Nenalezen zdroj odkazů.**

Po úspěšném zneplatnění je vytvořen protokol o zneplatnění certifikátu, který je prostřednictvím elektronické pošty zaslán pověřené osobě. Žadatel je o zneplatnění certifikátu informován prostřednictvím elektronické pošty na adresu uvedenou ve zneplatněném certifikátu (pokud certifikát adresu elektronické pošty obsahuje).

4.9.3.4 Zneplatnění certifikátu z vůle certifikační autority

O zneplatnění certifikátu může rozhodnout rovněž poskytovatel certifikačních služeb, pokud držitel certifikátu 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 prostřednictvím elektronické pošty neprodleně zaslán pověřené osobě společně s důvodem zneplatnění certifikátu.

Certifikační politika PostSignum Public CA pro komerční serverové certifikáty verze 1.1

Žadatel je o zneplatnění certifikátu informován prostřednictvím elektronické pošty na adresu uvedenou ve zneplatněném certifikátu (pokud certifikát adresu elektronické pošty obsahuje).

4.9.4 Doba odkladu požadavku na zneplatnění certifikátu

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

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

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

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

Uživatel certifikátu vydaného PostSignum Public CA (spoléhající se strana) je povinen postupovat v souladu s ustanoveními odst. 4.5.1.

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů (CRL) je vydáván vždy vzápětí po zpracování žádosti o revokaci certifikátu. Nedojde-li k revokaci certifikátu, je nový CRL vydáván alespoň každých 12 hodin. Seznam zneplatněných certifikátů je zveřejňován na třech místech:

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

Primárním zdrojem aktuálního CRL jsou webové stránky PostSignum VCA.

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

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

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

PostSignum VCA tuto službu neposkytuje.

Stav certifikátu je možné ověřit pouze na aktuálním CRL.

4.9.10 Požadavky při ověřování statutu certifikátu on-line

PostSignum VCA tuto službu neposkytuje.

Stav certifikátu je možné ověřit pouze na aktuálním CRL.

4.9.11 Jiné způsoby oznamování zneplatnění certifikátu

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

4.9.12 Případné odlišnosti postupu zneplatnění v případě kompromitace soukromého klíče

Postup pro zneplatnění certifikátu v případě kompromitace soukromého klíče je shodný s obecným postupem pro zneplatnění certifikátu.

4.9.13 Podmínky pro pozastavení platnosti certifikátu

PostSignum VCA tuto službu neposkytuje.

4.9.14 Subjekty oprávněné požadovat pozastavení platnosti certifikátu

PostSignum VCA tuto službu neposkytuje.

4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu

PostSignum VCA tuto službu neposkytuje.

4.9.16 Omezení doby pozastavení platnosti certifikátu

PostSignum VCA tuto službu neposkytuje.

4.10 Služby související s ověřováním statutu certifikátu

Status certifikátu je možné ověřit

- na seznamu zneplatněných certifikátů (CRL) v rámci služby umožňující přístup k veřejným informacím PostSignum VCA protokolem HTTP, nebo
- v rámci služby vyhledávání vydaných certifikátů přístupné na webových stránkách PostSignum.

4.10.1 Funkční charakteristiky

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

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

Primárním zdrojem aktuálního CRL jsou webové stránky PostSignum VCA.

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

4.10.2 Dostupnost služeb

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

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

4.10.3 Další charakteristiky služeb statutu certifikátu

Další charakteristiky služeb statutu certifikátu nejsou stanoveny.

**Certifikační politika PostSignum Public CA
pro komerční serverové certifikáty verze 1.1**

4.11 Ukončení poskytování služeb pro držitele certifikátu

Poskytování služeb pro držitele certifikátu končí ukončením smlouvy mezi zákazníkem a poskytovatelem certifikačních služeb. Toto se netýká služeb zneplatnění certifikátu, které jsou poskytovány po celou dobu platnosti certifikátu.

Ukončení smlouvy o poskytování certifikačních služeb nebo odstoupení od této smlouvy se řídí [VOP].

4.12 Úschova soukromého klíče u důvěryhodné třetí strany a jejich obnova

PostSignum VCA tuto službu neposkytuje.

4.12.1 Politika a postupy při úschově a obnovování soukromého klíče

PostSignum VCA tuto službu neposkytuje.

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

PostSignum VCA tuto službu neposkytuje.

5 MANAGEMENT, PROVOZNÍ A FYZICKÁ BEZPEČNOST

Pro PostSignum VCA byly zpracovány dokumenty:

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

Zmíněné dokumenty byly vypracovány na základě výsledků provedené analýzy rizik.

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

5.1 Fyzická bezpečnost

5.1.1 Umístění a konstrukce

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

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

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

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

5.1.2 Fyzický přístup

Pro každý typ pracoviště je v jeho provozním řádu definováno, kteří pracovníci mají na pracoviště fyzický přístup. Prostory jsou chráněny proti neoprávněnému vniknutí mechanickými prostředky (bezpečnostní zámky a mříže), na centrálním pracovišti též samostatnou smyčkou elektronického zabezpečovacího zařízení. Na pracoviště mobilní registrační autority se vztahují režimová opatření definovaná v Systémové bezpečnostní politice.

5.1.3 Elektřina a klimatizace

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

5.1.4 Vlivy vody

Centrální pracoviště jsou umístěna mimo zátopové oblasti.

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

5.1.5 Protipožární opatření a ochrana

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

5.1.6 Ukládání médií

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

5.1.7 Nakládání s odpady

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

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

5.1.8 Zálohy mimo budovu

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

5.2 Procesní bezpečnost

5.2.1 Důvěryhodné role

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

Zvláštní pozornost je zejména věnována při obsazování rolí s možností přístupu k centrálním systémům PostSignum VCA.

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

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

5.2.3 Identifikace a autentizace pro každou roli

Představitel každé role se musí při přístupu k prostředkům PostSignum VCA identifikovat a autentizovat. Každý uživatel má přidělenou jednoznačnou identifikaci ve všech systémech, ke

Certifikační politika PostSignum Public CA pro komerční serverové certifikáty verze 1.1

kterým má přístup. V systémech PostSignum VCA je používaná identifikace jménem resp. certifikátem a autentizace heslem resp. soukromým klíčem.

5.2.4 Role vyžadující rozdělení povinností

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

5.3 Personální bezpečnost

5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

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

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

5.3.2 Posouzení spolehlivosti osob

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

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

5.3.3 Požadavky na přípravu pro výkon role, vstupní školení

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

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

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

5.3.4 Požadavky a periodicita školení

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

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

5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Požadavky na rotaci pracovníků a její frekvenci nejsou definovány.

5.3.6 Postihy za neoprávněné činnosti zaměstnanců

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

5.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

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

5.3.8 Dokumentace poskytovaná zaměstnancům

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

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

5.4 Auditní záznamy (logy)

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

5.4.1 Typy zaznamenávaných událostí

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

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

5.4.2 Periodicita zpracování záznamů

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

5.4.3 Doba uchování auditních záznamů

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

5.4.4 Ochrana auditních záznamů

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

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

5.4.5 Postupy pro zálohování auditních záznamů

Auditní záznamy (kromě auditních záznamů o činnosti centrálních komponent certifikační autority v elektronické podobě) nejsou obecně zálohovány; jsou pouze archivovány. Důležité

Certifikační politika PostSignum Public CA pro komerční serverové certifikáty verze 1.1

auditní záznamy spojené s vydáním certifikátů jsou uchovávány ve dvou kopiích, které jsou uloženy v různých lokalitách.

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

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

5.4.7 Postup při oznamování události subjektu, který ji způsobil

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

5.4.8 Hodnocení zranitelnosti

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

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

5.5 Uchovávání informací a dokumentace

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

5.5.1 Typy informací a dokumentace, které se uchovávají

V PostSignum VCA se archivují tyto záznamy:

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

5.5.2 Doba uchování uchovávaných informací a dokumentace

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

5.5.3 Ochrana úložiště uchovávaných informací a dokumentace

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

5.5.4 Postupy při zálohování uchovávaných informací a dokumentace

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

5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

V PostSignum VCA nejsou časová razítka používána.

Certifikační politika PostSignum Public CA pro komerční serverové certifikáty verze 1.1

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

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

5.5.7 Postupy pro získání a ověření uchovávaných informací a dokumentace

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

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

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

5.6 Výměna dat pro ověřování elektronických značek v nadřazeném komerčním systémovém certifikátu poskytovatele

Platnost klíčů certifikačních autorit v hierarchii PostSignum VCA je omezena.

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

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

Plánovaná výměna klíčů certifikační autority musí být oznámena zákazníkům nejpozději 6 měsíců před vydáním nového certifikátu PostSignum Root QCA resp. 3 měsíce před uskutečněním výměny certifikátu autority PostSignum Public CA. Toto oznámení bude (včetně důvodu ukončení platnosti certifikátu) zveřejněno na webových stránkách PostSignum VCA a na všech pracovištích registrační autority PostSignum VCA.

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

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

5.7 Obnova po havárii nebo kompromitaci

Pro PostSignum VCA byly vypracovány dokumenty popisující zvládání krizových situací a postupy pro následnou obnovu.

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

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

5.7.1 Postup v případě incidentu a kompromitace

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

5.7.2 Poškození výpočetních prostředků, softwaru nebo dat

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

5.7.3 Postup při kompromitaci dat pro vytváření elektronických značek poskytovatele

5.7.3.1 Kompromitace soukromého klíče podřízené certifikační autority

V případě podezření na kompromitaci soukromého klíče PostSignum Public CA budou písemně nebo elektronicky informováni všichni držitelé certifikátů o mimořádném ukončení činnosti této autority; oznámení bude rovněž zveřejněno na webových stránkách PostSignum VCA, na všech pracovištích registrační autority PostSignum VCA a v jednom celostátně vydávaném deníku. Součástí oznámení bude i důvod ukončení platnosti certifikátu certifikační autority.

PostSignum Root QCA okamžitě zneplatní certifikát PostSignum Public CA a tato zneplatní všechny platné certifikáty vydané koncovým zákazníkům; zneplatněné certifikáty budou nejpozději do 12 hodin zveřejněny na příslušném CRL.

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

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

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

5.7.3.2 Kompromitace soukromého klíče PostSignum Root QCA

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

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

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

Certifikační politika PostSignum Public CA pro komerční serverové certifikáty verze 1.1

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

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

5.7.4 Schopnost obnovit činnost po havárii

Pokračování procesů certifikační autority po havárii závisí na typu havárie a jejích následcích.

V případě havárie malého a středního rozsahu přechází provoz PostSignum VCA do záložní lokality. Certifikační autorita je provozována v omezeném režimu, kdy pouze zajišťuje zneplatňování certifikátů a publikování CRL.

V případě havárie velkého rozsahu (přírodní pohroma, válečný stav), je obnova činnosti PostSignum VCA věcí rozhodnutí managementu České pošty. O rozhodnutí managementu musí být s minimální prodlevou informováni všichni zákazníci PostSignum VCA.

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

5.8 Ukončení činnosti CA nebo RA

5.8.1 Ukončení činnosti kořenové certifikační autority

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

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

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

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

5.8.2 Ukončení činnosti podřízené certifikační autority

Ukončení činnosti PostSignum Public CA musí být písemně oznámeno všem držitelům platných certifikátů a subjektům, které mají uzavřenou smlouvu přímo se vztahující k poskytování certifikačních služeb a rovněž zveřejněno na webových stránkách 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

Certifikační politika PostSignum Public CA pro komerční serverové certifikáty verze 1.1

certifikát vydaný PostSignum Public CA, musí tato autorita 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 této autority ukončena.

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

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

Následně ČP prokazatelně zničí data pro vytváření elektronických značek PostSignum Qualified CA, která sloužila pro podepisování kvalifikovaných certifikátů a seznamů zneplatněných certifikátů, a o tomto zničení provede záznam. Záznamy budou uchovávány v souladu s ustanoveními této certifikační politiky uvedenými v kapitole **Chyba! Nenalezen zdroj odkazů.**

5.8.3 Ukončení činnosti registrační autority

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

6 TECHNICKÁ BEZPEČNOST

6.1 Generování a instalace párových dat

Soukromé klíče žadatelů jsou generovány a uschovávány žadatelem o certifikát. Klíče mohou být generovány a následně i uloženy jak v softwarovém, tak i hardwarovém úložišti. Musí se jednat o klíče pro algoritmus RSA, s délkou modulu 1024 nebo 2048 bitů. PostSignum VCA nepředepisuje konkrétní požadavky na příslušné úložiště (není předepsáno používání prostředku pro bezpečné vytváření elektronických podpisů).

PostSignum VCA neposkytuje službu generování klíčů (párových dat) pro žadatele o certifikát. PostSignum VCA se soukromými klíči žadatelů nepřichází do styku, není zodpovědná za jejich ochranu ani zálohování.

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

6.1.1 Generování párových dat

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

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

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

6.1.2 Předání soukromého klíče

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

6.1.3 Předání veřejného klíče poskytovateli certifikačních služeb

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

6.1.4 Poskytování veřejného klíče certifikační autoritou spoléhajícím se stranám

Certifikáty certifikačních autorit a dále certifikáty, pro které byl vysloven souhlas se zveřejněním, jsou zveřejněny způsobem popsaným v kapitole 2.

6.1.5 Délky párových dat

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

Klíče držitelů certifikátů mají pro algoritmus RSA délku modulu 1024 a 2048 bitů. Jiný algoritmus než RSA není pro držitele certifikátů povolen.

6.1.6 Generování parametrů veřejného klíče a kontrola jejich kvality

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

Parametry používané při vytváření veřejných klíčů žadatelů o certifikát jsou generovány softwarovým nebo hardwarovým vybavením žadatele a poskytovatel certifikačních služeb za ně nenesou odpovědnost.

Kvalita parametrů klíčů generovaných v rámci PostSignum VCA je automaticky testována použitým programovým vybavením s výjimkou klíčů, které žadatel o certifikát generuje sám ve svém vlastním programovém vybavení.

6.1.7 Omezení pro použití veřejného klíče

Veřejné klíče koncových uživatelů mohou být použity pouze v souladu s pravidly popsanými v kapitole 1.4

6.2 Ochrana soukromého klíče a bezpečnost kryptografických modulů

6.2.1 Standardy a podmínky používání kryptografických modulů

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

6.2.2 Sdílení tajemství

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

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

6.2.3 Úschova soukromého klíče

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

6.2.4 Zálohování soukromého klíče

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

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

6.2.5 Uchovávání soukromého klíče

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

6.2.6 Transfer soukromého klíče do kryptografického modulu nebo z kryptografického modulu

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

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

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

6.2.7 Uložení soukromého klíče v kryptografickém modulu

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

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

6.2.8 Postup při aktivaci soukromého klíče

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

6.2.9 Postup při deaktivaci soukromého klíče

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

6.2.10 Postup při zničení soukromého klíče

Soukromý klíč certifikační autority uložený v HSM modulu je zničen prostředky poskytovanými HSM modulem v případě, že kryptografický modul má být dočasně použit k jiným účelům, v případě ukončení činnosti HSM modulu nebo v případě ukončení činnosti certifikační autority, jejíž klíče jsou v HSM modulu uloženy. Toto zničení soukromého klíče se provádí autorizovanou obsluhou v souladu s ustanoveními dokumentu Systémová bezpečnostní politika a dokumentu Provozní a bezpečnostní procedury nebo na základě požadavku Manažera VCA.

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

6.2.11 Hodnocení kryptografických modulů

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

6.3 Další aspekty správy párových dat

6.3.1 Uchovávání veřejných klíčů

Veřejné klíče ve formě certifikátů koncových uživatelů jsou archivovány v souladu s Auditní a archivační politikou.

6.3.2 Maximální doba platnosti certifikátu a párových dat

Doba platnosti certifikátu vydaného podle této certifikační politiky je jeden rok (přesně 365 dní). Páry klíčů svázané s certifikáty mají stejnou dobu platnosti jako certifikáty.

6.4 Aktivační data

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

6.4.1 Generování a instalace aktivačních dat

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

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

6.4.2 Ochrana aktivačních dat

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

6.4.3 Ostatní aspekty aktivačních dat

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

6.5 Počítačová bezpečnost

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Pro každou komponentu v hierarchii PostSignum VCA jsou definována nastavení zajišťující bezpečnost dané komponenty na technologické úrovni, který vycházejí ze standardů [CWA 141671] a [TS 101456].

6.5.2 Hodnocení počítačové bezpečnosti

Systém PostSignum VCA prošel po vybudování externí kontrolou bezpečnostní shody zaměřenou na splnění požadavků uvedených v [CWA 141671] a [TS 101456].

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

6.6 Bezpečnost životního cyklu

6.6.1 Řízení vývoje systému

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

Následné změny jsou realizovány v souladu s definovaným změnovým řízením.

6.6.2 Kontroly řízení bezpečnosti

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

6.6.3 Řízení bezpečnosti životního cyklu

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

6.7 Síťová bezpečnost

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

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

Veškerá komunikace mimo vyhrazené lokální sítě centrálních pracovišť je šifrovaná.

6.8 Časová razítka

V PostSignum VCA nejsou časová razítka používána.

7 PROFILY CERTIFIKÁTU, SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ A OCSP

7.1 Profil certifikátu

PostSignum VCA vydává certifikáty odpovídající standardu X.509. Profil komerčního serverového certifikátu je uveden v následující tabulce.

Tab. 2 Profil komerčního serverového certifikátu

Položka	Hodnota	Pov.	Změna	ORG	PFO	NFO
Version	3 (0x2)	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.				
Serial number	sériové číslo certifikátu přidělené certifikační autoritou					
SignatureAlgorithm	sha1WithRSAEncryption					
Issuer						
Country	CZ	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.				
Organisation	Česká pošta, s.p. [IČ 47114983] <i>uvedené číslo je IČ České pošty, s.p.</i>					
CN	PostSignum Public CA					
Validity						
Not Before	datum vydání, UTCTime	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.				
Not After	datum vydání + 365 dní, UTCTime					
Subject						
Country	CZ	ano	ne	X	X	X
Locality	trvalé bydliště fyzické osoby	ne	ne			X
Organisation	jméno právnické osoby nebo podnikající fyzické osoby ve tvaru: jméno zákazníka [IČ ič zákazníka]	ano	ano	X	X	
OU	rozlišující organizační jednotka právnické osoby nebo podnikající fyzické osoby, stanovená poskytovatelem certifikačních služeb	ne	ano	X	X	
OU	organizační jednotka, kde pracuje žadatel o certifikát nebo je zařízení provozováno	ne	ano	X	X	
OU	hodnota údaje serialNumber v případě nepodnikající fyzické osoby	ano	ne			X
CN	označení zařízení	ano	ne	X	X	X
serialNumber	jednoznačný identifikátor zákazníka přidělovaný poskytovatelem certifikačních služeb ve tvaru: <i>Sčíslo</i>	ano	ne	X	X	X
Subject Public Key Info						
Algorithm	rsaEncryption	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.				
SubjectPublicKey	veřejný klíč o velikosti 1024 nebo 2048 bitů					
Extensions	rozšíření certifikátu podle tabulky 3					
Signature	elektronická značka poskytovatele certifikačních služeb					

Vysvětlivky:

- Pov** povinná položka certifikátu
- Změna** položku je možné změnit v následném certifikátu
- ORG** položka je obsažena v certifikátech vydávaných zaměstnancům organizací
- PFO** položka je obsažena v certifikátech vydávaných podnikajícím fyzickým osobám
- NFO** položka je obsažena v certifikátech vydávaných nepodnikajícím fyzickým osobám

**Certifikační politika PostSignum Public CA
pro komerční serverové certifikáty verze 1.1**

7.1.1 Číslo verze

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

7.1.2 Rozšiřující položky v certifikátu

Rozšiřující položky použité v komerčním serverovém certifikátu jsou uvedeny v následující tabulce.

Tab. 3 Rozšíření v certifikátu

Položka	Hodnota	Pov.	Změna	ORG	PFO	NFO
Authority Key Identifier						
Key Identifier		Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.				
AuthorityCertIssuer						
AuthorityCertSerialNumber						
Subject Key Identifier						
Subject Alternative Name						
RFC822 Email address	e-mailová adresa žadatele	ne	ano	X	X	X
RFC822 Email address	e-mailová adresa žadatele	ne	ano	X	X	X
RFC822 Email address	e-mailová adresa žadatele	ne	ano	X	X	X
OtherName	identifikátor osoby přidělený zákazníkům položka „Description“ s OID: 2.5.4.13	ne	ano	X	X	X
Key Usage (kritické rozšíření)						
DigitalSignature	ano	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.				
NonRepudiation	ano					
KeyEncipherment	ano					
DataEncipherment	ne					
KeyAgreement	ne					
KeyCertSign	ne					
CRLSign	ne					
Certificate Policies						
Policy Identifier	2.23.134.1.2.1.8.110	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.				
Policy Qualifier id	CPS					
CPS URI	http://www.postsignum.cz					
CRL Distribution Points						
URI	http://www.postsignum.cz/crl/pspublicca.crl	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.				
URI	http://www2.postsignum.cz/crl/pspublicca.crl					
URI	http://postsignum.ttc.cz/crl/pspublicca.crl					
Basic Constraints	cA:FALSE					

Vysvětlivky:

Pov povinná položka certifikátu

Změna položku je možné změnit v následném certifikátu

ORG položka je obsažena v certifikátech vydávaných zaměstnancům organizací

PFO položka je obsažena v certifikátech vydávaných podnikajícím fyzickým osobám

NFO položka je obsažena v certifikátech vydávaných nepodnikajícím fyzickým osobám

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

Certifikační politika PostSignum Public CA pro komerční serverové certifikáty verze 1.1

Poznámka: Tato certifikační politika umožňuje vložit do certifikátu až 3 e-mailové adresy. Žadatel by si však měl předem ověřit, zda certifikát s více e-mailovými adresami podporují aplikace, ve kterých hodlá certifikát používat.

7.1.3 Objektové identifikátory (dále „OID“) algoritmů

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

7.1.4 Způsoby zápisu jmen a názvů

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

7.1.5 Omezení jmen a názvů

Jména a názvy uvedené v certifikátu musí přesně odpovídat údajům v dokladech, kterými zákazník nebo žadatel o certifikát prokazuje svoji totožnost. Za správnost údajů, které nejsou uvedené v předložených dokladech, odpovídá pověřená osoba zákazníka.

7.1.6 OID certifikační politiky

V každém certifikátu koncového uživatele je uveden odkaz na politiku, podle které byl certifikát vydán (OID politiky). OID této politiky je uvedeno v odstavci 1.2.

7.1.7 Rozšiřující položka „Policy Constraints“

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

7.1.8 Způsob zápisu kritické rozšiřující položky „Certificate Policies“

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

7.2 Profil seznamu zneplatněných certifikátů

Tab. 4 Profil CRL

Název položky	Hodnota/příznak použití
Version	2 (0x1)
Issuer Distinguished Name	
Country	CZ
Organisation	Česká pošta, s.p. [IČ 47114983]
CN	PostSignum Public CA
Validity	
This Update	Datum vydání, UTCTime
Next Update	Datum vydání + 12 hodin, UTCTime
RevokedCertificates	opakující se položka pro každý zneplatněný certifikát
UserCertificate	sériové číslo zneplatněného certifikátu
RevocationDate	datum a čas zneplatnění
CrlEntryExtensions	rozšíření položky CRL podle tabulky 5
CrlExtensions	rozšíření CRL podle tabulky 5
SignatureAlgorithm	sha1WithRSAEncryption
Signature	elektronická značka poskytovatele certifikačních služeb

**Certifikační politika PostSignum Public CA
pro komerční serverové certifikáty verze 1.1**

7.2.1 Číslo verze

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

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

Tab. 5 Rozšíření v CRL

Název rozšiřující položky	Hodnota/příznak použití	Kritická ano/ne
Rozšíření položky CrlEntryExtensions		
InvalidityDate	datum a čas vzniku události vedoucí ke zneplatnění certifikátu; volitelné rozšíření	ne
ReasonCode	důvod zneplatnění certifikátu	ne
Rozšíření CRL (CrlExtensions)		
Authority Key Identifier		ne
Key Identifier	používá se	
AuthorityCertIssuer	používá se	
AuthorityCertSerialNumber	používá se	
CRL Number	sériové číslo CRL přiřazené certifikační autoritou	ne

7.3 Profil OCSP

PostSignum VCA tuto službu neposkytuje.

7.3.1 Číslo verze

PostSignum VCA tuto službu neposkytuje.

7.3.2 Rozšiřující položky OCSP

PostSignum VCA tuto službu neposkytuje.

8 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

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

Součástí interní a externí kontroly je i kontrola bezpečnostní shody.

8.2 Identita a kvalifikace hodnotitele

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

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

8.3 Vztah hodnotitele k hodnocenému subjektu

Interní kontrolu provádí zaměstnanci České pošty, s. p.

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

8.4 Hodnocené oblasti

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

8.5 Postup v případě zjištění nedostatků

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

8.6 Sdělování výsledků hodnocení

O provedení každé kontroly je vypracována podepsaná písemná zpráva, která je předána manažerovi VCA. Ten zajistí její distribuci a projednání.

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

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

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

9.1.2 Poplatky za přístup k certifikátu na seznamu vydaných certifikátů

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

9.1.3 Poplatky za informace o statutu certifikátu nebo o zneplatnění certifikátu

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

9.1.4 Poplatky za další služby

Cena za další služby PostSignum VCA je stanovena v ceníku služeb České pošty, s. p., který je mj. dostupný na webových stránkách PostSignum VCA.

9.1.5 Jiná ustanovení týkající se poplatků (vč. refundací)

Žádná ustanovení v tomto odstavci.

9.2 Finanční odpovědnost

9.2.1 Krytí pojištěním

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

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

9.2.2 Další aktiva a záruky

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

Výroční zpráva je k nahlédnutí též na webových stránkách České pošty (www.cpost.cz).

9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

PostSignum VCA tuto službu neposkytuje.

9.3 Citlivost obchodních informací

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

9.3.1 Výčet citlivých informací

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

9.3.2 Informace mimo rámec citlivých informací

Za důvěrné se 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 v komerčním certifikátu, pokud k jeho zveřejnění dal držitel souhlas.

9.3.3 Odpovědnost za ochranu citlivých informací

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

9.4 Ochrana osobních údajů

Česká pošta zajišťuje ochranu osobních údajů osob, k nimž získá přístup při poskytování certifikačních služeb. Zásady ochrany osobních údajů jsou obsaženy v této certifikační politice, [VOP] a v Certifikační prováděcí směrnici a vycházejí z příslušných ustanovení [Z101].

9.4.1 Politika ochrany osobních údajů

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

9.4.2 Osobní údaje

Za osobní údaje jsou považovány informace, které spadají pod ochranu [Z101]. Zejména se jedná o veškeré informace týkající se určené nebo určitelné fyzické osoby (zákazníka – podnikající a nepodnikající fyzické osoby, pověřené osoby nebo žadatele).

9.4.3 Údaje, které nejsou považovány za citlivé

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

9.4.4 Odpovědnost za ochranu osobních údajů

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

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

Žadatel o certifikát dává během procesu vydání prvního certifikátu České poště souhlas se zpracováním svých osobních údajů. Žadatel o certifikát dále dává České poště souhlas se zpracováním svého rodného čísla.

9.4.6 Poskytnutí citlivých informací pro soudní či správní účely

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.

9.4.7 Jiné okolnosti zpřístupňování osobních údajů

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

9.5 Práva duševního vlastnictví

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

9.6 Zastupování a záruky

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

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

9.6.1 Zastupování a záruky CA

Viz ustanovení odst. 9.6.

9.6.2 Zastupování a záruky RA

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

Jinak viz ustanovení odst. 9.6.

9.6.3 Zastupování a záruky držitele certifikátu

Zákazník (držitel certifikátu) nebo žadatel ručí za naplnění všech povinností zákazníků a žadatelů o certifikát uvedených v této certifikační politice.

9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strana ručí za naplnění všech povinností, které jsou na spoléhající se stranu kladeny před použitím komerčního certifikátu. Tyto povinnosti jsou uvedeny v této certifikační politice, především v odst. 4.5.1.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

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

9.7 Zřeknutí se záruk

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

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

Česká pošta neodpovídá za škodu vyplývající z použití komerčního systémového certifikátu, pokud došlo ze strany držitele a nebo spoléhající se osoby k nedodržení omezení pro jeho použití, uvedených v této certifikační politice a zveřejněných na webové stránce PostSignum VCA.

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

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

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

9.9 Odpovědnost za škodu, náhrada škody

Pokud nevyplývá z 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.

9.10 Doba platnosti, ukončení platnosti

9.10.1 Doba platnosti

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

9.10.2 Ukončení platnosti

Platnost dokumentu je ukončena v případě

- jeho nahrazení novější verzí, nebo

Certifikační politika PostSignum Public CA
pro komerční serverové certifikáty verze 1.1

- ukončení poskytování služeb Českou poštou, s. p. jako poskytovatelem certifikačních služeb.

9.10.3 Důsledky ukončení a přetrvání závazků

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

9.11 Komunikace mezi zúčastněnými subjekty

9.11.1 Komunikace s poskytovatelem certifikačních služeb

Veškeré informace, které chce poskytovatel certifikačních služeb sdělit zákazníkům, zveřejní na svých webových stránkách a na vývěskách na pracovištích registračních autorit. Závažné informace, jako například podezření na kompromitaci klíče některé z certifikačních autorit hierarchie PostSignum, sděluje poskytovatel certifikačních služeb opět na webových stránkách a současně písemným nebo elektronickým upozorněním směřovaným na zákazníky.

Zákazník – organizace komunikuje s poskytovatelem certifikačních služeb prostřednictvím pověřené osoby. Pověřená osoba se obrací na pracoviště registrační autority nebo na regionální obchodní místa.

Zákazník – podnikající nebo nepodnikající fyzická osoba komunikuje s poskytovatelem certifikačních služeb osobně. Obrací se na pracoviště registrační autority nebo na regionální obchodní místa.

Komunikace zákazníka s poskytovatelem certifikačních služeb může probíhat rovněž elektronicky. V případě požadavku na právní prokazatelnost elektronické komunikace musí být tato založena na certifikátech vydaných PostSignum VCA nebo jinou autoritou, kterou Česká pošta označí za důvěryhodnou, a o akceptaci jejíhož certifikátu se se zákazníkem předem písemně dohodne formou dodatku ke smlouvě.

9.11.2 Komunikace v rámci systému PostSignum VCA

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

9.11.3 Komunikační jazyk

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

9.12 Změny

9.12.1 Postup při změnách

Postupy pro zapracování změn jsou uvedeny v odst. 1.5.

9.12.2 Postup při oznamování změn

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

Držitelé certifikátů se mohou na webových stránkách PostSignum VCA přihlásit k odebírání e-mailového zpravodaje, kterým bude mj. oznamováno vydání nové verze certifikační politiky.

Certifikační politika PostSignum Public CA pro komerční serverové certifikáty verze 1.1

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

9.12.3 Okolnosti, při kterých musí být změněn OID

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

OID jsou přiřazeny:

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

OID nejsou přiřazeny registračním autoritám ani certifikační prováděcí směrnici.

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

9.13 Řešení sporů

V případě vzniku sporu mezi zákazníkem a PostSignum VCA se zákazník obrátí na

- manažera VCA, nebo
- registrační autoritu (formou žádosti o reklamaci).

Pokud ani jedna z výše uvedených instancí nesjedná ukončení sporu, bude se spor mezi zákazníkem a PostSignum VCA řešit u místně a věcně příslušného soudu.

9.14 Rozhodné právo

Činnost PostSignum VCA se řídí právním řádem České republiky.

9.15 Shoda s právními předpisy

Činnost PostSignum VCA je v souladu s právním řádem České republiky.

Vztah mezi Českou poštou, s.p. a zákazníkem je upraven písemnou smlouvou o poskytování certifikačních služeb.

9.16 Další ustanovení

9.16.1 Rámcová dohoda

Žádná ustanovení v tomto odstavci.

9.16.2 Postoupení práv

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

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

**Certifikační politika PostSignum Public CA
pro komerční serverové certifikáty verze 1.1**

9.16.3 Oddělitelnost ustanovení

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

9.16.4 Zřeknutí se práv

Žádná ustanovení v tomto odstavci.

9.16.5 Vyšší moc

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

9.17 Další opatření

9.17.1 Řídící dokumenty

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

- | | |
|--------------|--|
| [CWA 141671] | CWA 14167-1:2003: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements |
| [ISO 27001] | ČSN ISO/IEC 27001:2006 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky |
| [TS 101456] | ČSN ETSI TS 101 456 Elektronické podpisy a infrastruktury; Požadavky na postupy certifikační autority vydávající komerční certifikáty, verze 1.3.1 |
| [TR 13335] | ČSN ISO/IEC TR 13335: Informační technologie – Směrnice pro řízení bezpečnosti IT |
| [ISO 17799] | ČSN ISO/IEC 17799: Informační technologie – Bezpečnostní techniky Soubor postupů pro management bezpečnosti informací RFC 2511 – Internet X.509 Certificate Request Message Format |
| [RFC 3280] | Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile |
| [RFC 5280] | Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile |
| [RFC 3647] | Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework |
| [RFC 3739] | Internet X.509 Public Key Infrastructure: Public Certificates Profile |
| [V378] | Vyhláška Ministerstva informatiky č. 378/2006 Sb. ze dne 19. července 2006 o postupech komerčních poskytovatelů certifikačních služeb |
| [Z101] | Zákon č. 101/2000 Sb. o ochraně osobních údajů v aktuálním znění |
| [ZoEP] | Zákon č. 227/2000 Sb. o elektronickém podpisu v platném znění |

**Certifikační politika PostSignum Public CA
pro komerční serverové certifikáty verze 1.1**

9.17.2 Odkazy a literatura

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