CERTIFIKAČNÍ PROVÁDĚCÍ SMĚRNICE PRO ÚLOHU VEŘEJNÁ CERTIFIKAČNÍ AUTORITA ČESKÉ POŠTY, S.P.

Praha, září 2006

1. ÚVOD

Tato certifikační prováděcí směrnice upravuje postupy činnosti certifikační autority PostSignum VCA související s vydáváním komerčních certifikátů podle všech platných certifikačních politik.

1.1 Obecný přehled

Česká pošta, s.p. (dále i Česká pošta či ČP), jako poskytovatel certifikačních služeb, ustavila certifikační autoritu PostSignum Public CA (dále i PostSignum VCA), které vydala certifikát certifikační autorita PostSignum Root QCA. PostSignum Public CA vydává certifikáty koncových uživatelů

Tato Certifikační prováděcí směrnice (dále i jen CPS) doplňuje nebo rozvádí vybraná témata jednotlivých certifikačních politik (dále i CP) a upravuje tak vydávání certifikátů certifikační autoritou PostSignum VCA. V případě rozporu mezi CPS a certifikační politikou, která se na toto CPS odkazuje, platí ustanovení certifikační politiky.

Certifikační autorita PostSignum VCA byla vybudována a je provozována v souladu s obecně uznávanými standardy v oblasti PKI.

Tato CPS poskytuje věcné informace popisující

- postupy užívané při poskytování certifikačních služeb,
- technologie, procesy a provozní podmínky, které poskytování certifikačních služeb umožňují.

Postupy popsané v této CPS spolu s technologiemi a procesy popsanými v dalších dokumentech dokumentují postupy a pravidla vedoucí k zajištění důvěryhodnosti a integrity certifikační autority PostSignum VCA při poskytování certifikačních služeb, jakož i důvěryhodnosti certifikátů, které jsou PostSignum VCA vydávány, a to od okamžiku vydání certifikátu až po vypršení jeho platnosti.

1.1.1 Certifikační služby poskytované PostSignum VCA

Certifikační služby nabízené certifikační autoritou PostSignum VCA jsou uvedeny v příslušných certifikačních politikách v níže uvedeném rozsahu:

PostSignum VCA poskytuje služby v plném rozsahu popsaném v níže uvedených certifikačních politikách, podle nichž jsou vydávány certifikáty pro koncové zákazníky:

- Certifikační politika PostSignum Public CA pro certifikáty zaměstnanců nebo podnikající fyzické osoby verze 1.60 vydaná 1.9.2006,
- Certifikační politika PostSignum Public CA pro šifrovací certifikáty skupin osob verze 1.60 vydaná 1.9.2006,
- Certifikační politika PostSignum Public CA pro certifikáty technologických komponent organizací verze 1.60 vydaná 1.9.2006,

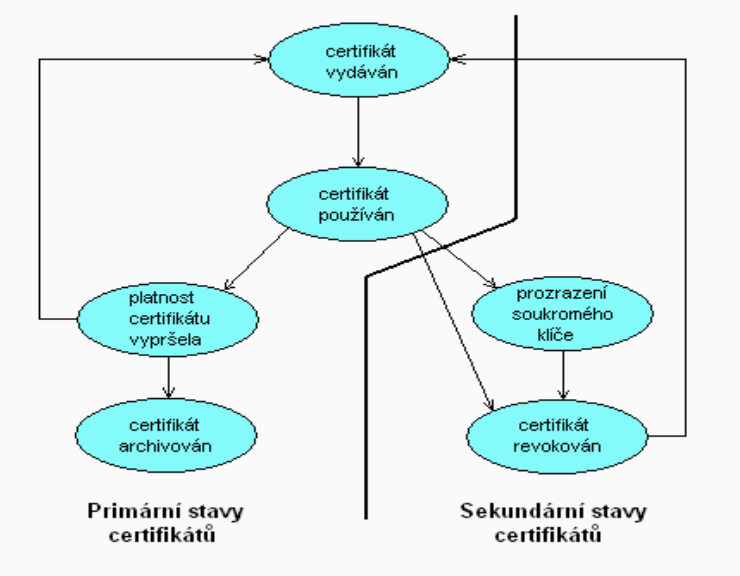
- Certifikační politika PostSignum Public CA pro certifikáty fyzických osob verze 1.20 vydaná 1.9.2006,

- Certifikační politika PostSignum Public CA pro certifikáty technologických komponent fyzických osob verze 1.20 vydaná 1.9.2006.

1.1.2 Životní cyklus certifikátu

Životní cyklus certifikátů vydávaných PostSignum VCA je znázorněn na Obr.1

Obr.1 Životní cyklus certifikátu



Obr.1 reprezentuje na nejvyšší úrovni správu certifikátů v rámci PostSignum VCA. Certifikát může být v některém z primárních nebo sekundárních stavů. Rozeznáváme tyto primární stavy certifikátů:

- certifikát vydáván,

- certifikát používán,

- platnost certifikátu vypršela,

- certifikát archivován.

Všechny certifikáty vydané PostSignum VCA procházejí těmito primárními stavy.

Sekundární stavy certifikátu jsou tyto:

- prozrazení soukromého klíče,

- certifikát revokován.

Sekundární stavy představují výjimečné situace, proto se předpokládá, že

- většina certifikátů vydaných PostSignum VCA projde ve svém životním cyklu pouze primárními stavy,

- pouze malá část certifikátů vydaných PostSignum VCA projde ve svém životním cyklu některým ze sekundárních stavů.

PostSignum VCA podporuje všechny uvedené stavy certifikátů, avšak nepodporuje žádné dočasné stavy, jako například pozastavení platnosti certifikátu.

1.2 Identifikace dokumentu

Tab. 1 Identifikace CPS

Název dokumentu	Certifikační prováděcí směrnice PostSignum VCA
Verze dokumentu	1.40
Stav	finální
OID PostSignum Root QCA	2.23.134.1.4.2.1
OID tohoto CPS	Není přidělováno
Datum vydání	1.9.2006
Doba platnosti	do odvolání

1.3 Revize dokumentu

Tato CPS je pravidelně revidována tak, jak předepisuje Komise pro certifikační politiky ČP. Jednotlivé verze dokumentu jsou označeny číslem verze, které umožňuje danou verzi identifikovat.

1.4 Zúčastněné strany a oblast použití

Česká pošta, s.p., jako poskytovatel certifikačních služeb, ustavila certifikační autoritu PostSignum Public CA (dále i PostSignum VCA), které vydala certifikát certifikační autorita PostSignum Root QCA. PostSignum VCA je řízena a provozována Českou poštou, s.p.

Tato certifikační prováděcí směrnice se týká

- všech certifikačních služeb, které jsou poskytovány certifikační autoritou PostSignum VCA,

- všech certifikátů, které byly vydány certifikační autoritou PostSignum VCA,

- všech subjektů, které s vydanými certifikáty pracují nebo se na tyto spoléhají.

1.4.1 Poskytovatel certifikačních služeb

Poskytovatelem certifikačních služeb je

Česká pošta, s.p.

IČ 47114983, DIČ CZ47114983

Olšanská 38/9

225 99 Praha 3

tel. 267 196 111

1.4.2 Hlavní dodavatel

Hlavním dodavatelem certifikační autority PostSignum VCA je

ICZ, a.s.

IČ 25145444

Hvězdova 1689/2a

140 00 Praha 4

tel.: 244 100 111

fax: 244 100 222

1.4.3 Certifikační autority

1.4.3.1 PostSignum Root QCA

PostSignum Root QCA vydala certifikát pro certifikační autoritu PostSignum VCA. Bezpečnostní opatření, jimiž je PostSignum Root QCA chráněna, jsou přiměřená významu této certifikační autority.

1.4.3.2 Funkce PostSignum Root QCA

PostSignum Root QCA zajišťuje zejména tyto funkce:

- generování vlastních klíčů,
- vydání samopodepsaného kvalifikovaného systémového certifikátu,
- zveřejnění vlastního kvalifikovaného systémového certifikátu v adresářových službách PostSignum QCA, na webových stránkách PostSignum QCA a dalšími vhodnými způsoby,
- poskytování informací o vydaných certifikátech,
- provozování certifikačních služeb v souladu s dokumentovanými provozními postupy,
- stanovení jmenných konvencí pro podřízené certifikační autority v souladu se standardem X.520 pro rozlišovací jména,
- administrativu spojenou s registrací žadatelů o certifikát,
- vydání kvalifikovaných systémových certifikátů pro podřízené certifikační autority,
- revokaci certifikátů podle pravidel stanovených v certifikačních politikách,
- prověřování případů podezření, že došlo k prozrazení soukromého klíče certifikační autority,

- zveřejňování seznamů zneplatněných certifikátů v adresářových službách a jiným vhodným způsobem,

- asistovat při kontrole, kterou provádí externí auditor nebo pověřený pracovník České pošty.

1.4.3.3 Certifikační autorita PostSignum VCA

Hlavním úkolem PostSignum VCA je vydávat a spravovat certifikáty pro zákazníky České pošty v souladu s definovanými certifikačními politikami.

1.4.3.4 Funkce PostSignum VCA

Certifikační autorita PostSignum Public CA zajišťuje především tyto funkce:

- generování vlastního páru klíčů,

- podání žádosti o certifikát u PostSignum Root QCA,

- zveřejnění všech certifikačních politik, podle kterých vydává certifikáty, na webových stránkách PostSignum VCA,

- provozování certifikačních služeb v souladu s dokumentovanými provozními postupy,

- administrativu spojenou s registrací žadatelů o certifikát,

- vydání certifikátů pro koncové subjekty (subjekty, které nejsou certifikačními autoritami), registrační autority a technologické komponenty, které jsou součástí dané certifikační autority,

- revokaci certifikátů podle pravidel stanovených v certifikačních politikách,

- prověřování případů podezření, že došlo k prozrazení soukromého klíče certifikační autority,

- zveřejňování vydaných certifikátů, s jejichž zveřejněním dal držitel souhlas, v adresářových službách PostSignum VCA a jiným vhodným způsobem,

- zveřejňování seznamů zneplatněných certifikátů v adresářových službách PostSignum VCA a jiným vhodným způsobem,

- asistovat při kontrole, kterou provádí externí auditor nebo pověřený pracovník České pošty.

1.4.4 Registrační autority

Registrační autority zajišťují zejména tyto funkce:

- participují na certifikačních službách v souladu s dokumentovanými provozními postupy,

- registrují žádosti o certifikát, přijímají je nebo zamítají v souladu s platnými certifikačními politikami,

- zajišťují předání vydaného certifikátu žadateli,

- ověřují totožnost žadatelů o certifikát,
- vedou evidenci žádostí o certifikát, které byly jejich prostřednictvím podány,
- revokují certifikáty podle platných certifikačních politik,
- prověřují případy podezření, že došlo k prozrazení soukromého klíče registrační autority,
- asistovat při kontrole, kterou provádí externí auditor nebo pověřený pracovník České pošty.

1.4.5 Zákazníci

Zákazníkem PostSignum VCA je fyzická či právnická osoba, která uzavírá písemnou smlouvu o poskytování certifikačních služeb s Českou poštou. Certifikáty jsou vydávány

- organizacím, které uzavírají s Českou poštou smlouvu o poskytování certifikačních služeb,
- fyzickým osobám - jednotlivcům, kteří uzavírají s Českou poštou smlouvu o poskytování certifikačních služeb.

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

1.4.5.1 Oprávněná osoba

Oprávněnou osobou je osoba definovaná zákazníkem - organizací 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 - politiky, podle které bude certifikát vydán).

Česká pošta získá při uzavírání smlouvy ověřený podpisový vzor oprávněné osoby.

1.4.5.2 Žadatel

Žadatel o certifikát je zaměstnanec zákazníka - organizace nebo fyzická osoba, která má právo žádat o certifikát podle některé z platných certifikačních politik.

1.4.6 Uživatelé certifikátů PostSignum VCA a další zúčastněné strany

Uživatelem certifikátu je libovolná fyzická či právnická osoba spoléhající se na certifikát vydaný PostSignum VCA. Uživatelé certifikátu nevstupují do smluvního vztahu s poskytovatelem certifikačních služeb.

1.4.7 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 PostSignum VCA. Jedná se o politiky pro certifikační autoritu PostSignum Public CA.

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.

1.4.7.1 Povinnosti a zodpovědnost PAA ČP

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 publikaci platných politik,
- zodpovídá za konzistenci a integritu politik,
- schvaluje veškeré změny CPS,
- zodpovídá za publikování aktuální verze CPS,
- zodpovídá za konzistenci a integritu CPS.

1.5 Použitelnost certifikátů

Certifikáty PostSignum VCA mohou být použity k zajištění služby digitálního podpisu, autentizace a šifrování.

Podrobnější popis použití certifikátu je uveden v příslušné certifikační politice.

1.6 Správa dokumentů

1.6.1 Správce dokumentu

Za správu této certifikační prováděcí směrnice a za její soulad s certifikačními politikami odpovídá manažer VCA.

1.6.2 Správa certifikačních politik a certifikační prováděcí směrnice

Tento dokument je vytvářen týmem pro tvorbu certifikačních politik ČP (Policy Creation Authority - PCA ČP), který je rovněž zodpovědný za tvorbu certifikačních politik. 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 předloží manažer VCA Komisi pro certifikační politiky jejich přehled; Komise pro certifikační politiky rozhodne, jakým způsobem budou plánované změny zveřejněny. Manažer VCA pak předá požadavek týmu pro tvorbu certifikačních politik (PCA ČP) a vypracované politiky nebo CPS předloží ke schválení Komisi pro certifikační politiky.

Při inicializaci vytvoření nové certifikační politiky nebo CPS sdělí manažer VCA Komisi pro certifikační politiky požadavek na vytvoření nové politiky nebo CPS včetně seznamu požadavků na tyto dokumenty a v případě politik OID. Komise pro certifikační politiky podle potřeby ustanoví PCA ČP. Manažer VCA pak předá požadavek týmu pro tvorbu certifikačních politik (PCA ČP) a vypracované politiky nebo CPS předloží ke schválení Komisi pro certifikační politiky, která potom potvrdí OID a přidělí číslo verze.

1.6.3 Změny v certifikační prováděcí směrnici

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

Veškeré změny v této certifikační prováděcí směrnici podléhají schválení Komise pro certifikační politiky ČP (PAA ČP). PAA ČP přidělí nové číslo verze.

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

1.6.4 Platnost

Platnost tohoto dokumentu je uvedena v kapitole 1.2.

1.6.5 Ukončení platnosti

Platnost tohoto dokumentu je ukončena nejpozději dnem ukončení služeb autority PostSignum VCA.

1.7 Kontaktní údaje

1.7.1 Poskytovatel certifikačních služeb

Poskytovatelem certifikačních služeb je

Česká pošta, s.p., IČ 47114983

se sídlem

Olšanská 38/9, 225 99 Praha 3

tel. 267 196 111

1.7.2 Kontaktní osoba

Kontaktní osobou poskytující informace o PostSignum VCA je manažer VCA. Další informace o PostSignum VCA získáte na adrese

http://www.postsignum.cz

nebo u manažera VCA

manager.postsignum@cpost.cz

1.7.3 Osoba zodpovědná za soulad certifikačních politik a CPS

Osobou zodpovědnou za soulad CPS a certifikačních politik v rámci PostSignum VCA je manažer VCA, kterého lze kontaktovat na adrese uvedené v odstavci 1.7.2.

1.7.4 Komise pro certifikační politiky České pošty

Kontaktní údaje Komise pro certifikační politiky ČP jsou uvedeny v každé certifikační politice, kterou tato komise schválila.

1.7.5 Kontaktní údaje PostSignum Root QCA

Kontaktní údaje PostSignum Root QCA jsou uvedeny a zveřejněny v každé certifikační politice PostSignum VCA.

1.7.6 Kontaktní údaje PostSignum VCA

Kontaktní údaje PostSignum VCA jsou uvedeny a zveřejněny v každé certifikační politice, podle které certifikační autorita PostSignum VCA vydává certifikáty, a na webových stránkách PostSignum VCA.

1.7.7 Kontaktní údaje registračních autorit

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

1.8 Použité zkratky a pojmy

Předpokládá se, že osoba seznamující se s touto certifikační prováděcí směrnicí má základní znalosti z oblasti PKI, včetně

- použití digitálních podpisů pro zjištění autentizace, integrity a nepopiratelnosti,
- principů asymetrické kryptografie a certifikátů veřejných klíčů,
- rolí certifikační a registrační autority.

1.8.1 Použité zkratky a pojmy

VCA ČP - viz. PostSignum VCA

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.

Certifikát – certifikát ve smyslu zákona o elektronickém podpisu [ZoEP].

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

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

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

Následný certifikát - certifikát vydaný na základě uzavřené smlouvy jako náhrada za již vydaný certifikát PostSignum Public CA; údaje v položce Subject následného certifikátu musí být shodné s údaji v certifikátu, který je nahrazován. Pro vydání následného certifikátu není vyžadovaná 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.

PostSignum VCA - označení pro informační systém certifikační autority PostSignum Public CA.

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

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

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

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

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

Rozlišovací jméno - jednoznačně identifikuje žadatele o certifikát resp. držitele certifikátu dle pravidel definovaných příslušnou certifikační politikou.

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

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

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

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

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

Zákazník - fyzická osoba - nepodnikající osoba bez přiřazeného identifikačního čísla.

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

2. ZVEŘEJŇOVÁNÍ A UCHOVÁVÁNÍ INFORMACÍ

2.1 Uložení dat, jejich správa a zásady zveřejňování

Vydané certifikáty jsou uloženy v adresářových službách PostSignum VCA a v databázi certifikační autority.

Informace o vydaných certifikátech a jejich stavu (prostřednictvím seznamu zneplatněných certifikátů - CRL) jsou poskytovány přes adresářové služby a na webových stránkách PostSignum VCA.

Bližší informace o uložení dat, jejich správě a zásadách zveřejňování jsou uvedeny v příslušné certifikační politice.

2.2 Zveřejňování informací o certifikační autoritě

Informace o zveřejňování informací o certifikační autoritě jsou uvedeny v příslušné certifikační politice.

2.3 Periodicita zveřejňování

Informace o periodicitě zveřejňování jsou uvedeny v každé certifikační politice.

2.4 Řízení přístupu k informacím

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

Bližší informace o přístupu k informacím poskytovaným PostSignum VCA jsou uvedeny v každé certifikační politice.

3. IDENTIFIKACE A AUTENTIZACE

3.1 Struktura a přidělování jmen

3.1.1 Typy jmen uvedených v certifikátu

Vzhledem k tomu, že PostSignum VCA vydává certifikáty pro různé subjekty podle různých certifikačních politik, nelze souhrnně a obecně definovat údaje o typech jmen uvedených v certifikátu. Tyto údaje jsou definovány v každé certifikační politice.

3.1.2 Věcná správnost jmen

Vzhledem k tomu, že PostSignum VCA vydává certifikáty pro různé subjekty podle různých certifikačních politik, nelze souhrnně a obecně definovat požadavky na věcnou správnost jmen. Tyto údaje jsou uvedeny v každé certifikační politice.

3.1.3 Pravidla interpretace různých forem jmen

Vzhledem k tomu, že PostSignum VCA vydává certifikáty pro různé subjekty podle různých certifikačních politik, nelze souhrnně a obecně definovat pravidla interpretace různých forem jmen. Tyto údaje jsou uvedeny v každé certifikační politice.

3.1.4 Transkripce údajů, znakové sady

3.1.4.1 PostSignum Root QCA

Pravidla pro PostSignum Root QCA jsou definována v Certifikační prováděcí směrnici PostSignum QCA.

3.1.4.2 PostSignum Public CA

V certifikátech vydávaných certifikační autoritou PostSignum VCA jsou podporovány pouze následující znakové sady:

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

Veškeré údaje dokladované zákazníkem nebo žadatelem při registraci žádosti o certifikát se do certifikátů vydávaných PostSignum Public CA přenášejí ve tvaru, ve kterém jsou uvedeny v předkládaných dokladech a průkazech totožnosti, nebo ve tvaru, který je kódován znakovou sadou neobsahující české znaky a je přesnou transkripcí bez diakritiky údajů v předkládaných dokladech a průkazech totožnosti.

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

3.1.5 Jednoznačnost jmen

Vzhledem k tomu, že PostSignum VCA vydává certifikáty pro různé subjekty podle různých certifikačních politik, nelze souhrnně a obecně definovat způsob, jakým má být zajištěna jedinečnost jmen. Tyto údaje jsou uvedeny v každé certifikační politice.

Obecně však platí, že PostSignum VCA nepřiřadí stejné rozlišovací jméno dvěma různým subjektům. Může však vydat dva i více certifikátů se stejným rozlišovacím jménem v položce Subject, avšak vždy se jedná o certifikát pro stejný subjekt, což je zaručeno v souladu s certifikační politikou, dle které je certifikát vydán.

3.1.6 Postup v případě kolize jmen

Vzhledem k tomu, že PostSignum VCA vydává certifikáty pro různé subjekty podle různých certifikačních politik, nelze souhrnně a obecně definovat, jaký je postup v případě kolize jmen. Tyto údaje jsou uvedeny v každé certifikační politice.

Obecně však platí, že PostSignum VCA nepřiřadí stejné jméno dvěma různým subjektům. Může však vydat dva i více certifikátů se stejným rozlišovacím jménem v položce Subject, avšak vždy se jedná o certifikát pro stejný subjekt, což je zaručeno postupem popsaným v certifikační politice, dle které je certifikát vydán.

V případě, kdy přes všechna opatření dojde ke kolizi jmen, bude tento problém postoupen manažerovi VCA, který ve spolupráci se zúčastněnými zákazníky sjedná nápravu.

3.2 Pre-registrace

3.2.1 Způsob ověření vazby mezi soukromým a veřejným klíčem zákazníka

Žadatel předkládá registrační autoritě elektronickou žádost o certifikát ve formátu PKCS#10, kde jsou uvedeny údaje o subjektu, pro který má být vydán certifikát, včetně veřejného klíče subjektu. Tyto údaje spolu s veřejným klíčem jsou digitálně podepsány soukromým klíčem. Registrační autorita ověřuje digitální podpis žádosti. Pokud je podpis ověřen jako platný, má se za to, že žadatel vlastní soukromý klíč odpovídající veřejnému klíči, který bude uveden v certifikátu.

3.2.2 Způsob prokázání identity organizace

Identita organizace se prokazuje při uzavírání smlouvy o poskytování certifikačních služeb způsobem obvyklým v obchodním styku.

3.2.3 Uzavření smlouvy se zákazníkem - organizací

3.2.3.1 Pre-registrace žadatelů o certifikát u zákazníka - organizace

Registrační autorita PostSignum VCA ověřuje fyzicky totožnost žadatelů pomocí standardních osobních dokladů. Protože v certifikátu jsou uváděny rovněž údaje o organizaci, ke které žadatel patří, operátor registrační autority PostSignum VCA musí ověřit i tuto vazbu.

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

Oprávněná osoba zasílá nebo předává poskytovateli certifikačních služeb seznam žadatelů, kteří mohou žádat o certifikát podle určité certifikační politiky. Seznam je podepsán oprávněnou osobou.

První pre-registrace může též proběhnout

- při přípravě smlouvy a příloh na obchodním místě, v tomto případě se pre-registrace stává platnou až po podpisu smlouvy nebo

- při podpisu smlouvy na registrační autoritě, na registrační autoritě je však možné pre-registrovat pouze žadatele o certifikáty podle politiky pro vydávání certifikátů zaměstnanců.

3.2.3.2 Způsob prokázání zmocnění k podepisování za organizaci

Zmocnění k podepisování za organizaci se prokazuje při uzavírání smlouvy o poskytování certifikačních služeb způsobem obvyklým v obchodním styku.

3.2.3.3 Změna oprávněné osoby

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

3.2.3.4 Způsob prokázání totožnosti zaměstnance zákazníka

Zaměstnanec prokazuje svou totožnost svým osobním dokladem. Výčet osobních dokladů akceptovaných registrační autoritou je uveden v certifikační politice, podle níž je zaměstnanci vydán certifikát. Registrační autorita zkontroluje

- zda je doklad platný,

- zda fotografie na dokladu odpovídá zaměstnanci.

V certifikační politice mohou být stanoveny další požadavky na kontrolu, jako například doložení identity jiným způsobem, existence záznamu o daném žadateli v evidenci oprávněných žadatelů atd.

3.2.4 Uzavření smlouvy se zákazníkem - fyzickou osobou

Zákazník se dostaví na registrační autoritu a požádá o vydání certifikátu pro fyzickou osobu. Dále obsluze registrační autority předá své identifikační údaje, včetně adresy bydliště, nezbytné pro uzavření smlouvy. Tyto údaje doloží způsobem určeným danou certifikační politikou.

Obsluha registrační autority připraví jednorázovou smlouvu na vydání certifikátu a spolu se zákazníkem ji podepíše.

3.2.4.1 Způsob prokázání totožnosti fyzické osoby

Fyzická osoba prokazuje svou totožnost jedním osobním dokladem a jedním doplňujícím dokladem. Výčet osobních a doplňujících dokladů akceptovaných registrační autoritou je uveden v certifikační politice, podle níž je fyzické osobě vydán certifikát. Registrační autorita zkontroluje

- zda jsou doklady platné,
- zda fotografie na dokladech odpovídá fyzické osobě.

V certifikační politice mohou být stanoveny další požadavky na kontrolu, jako například doložení identity jiným způsobem, existence záznamu o daném žadateli v evidenci oprávněných žadatelů atd.

3.2.5 Podmínky uzavření smlouvy

Česká pošta uzavírá se zákazníkem smlouvu o poskytování certifikačních služeb za podmínek definovaných obchodním zákoníkem.

3.3 Žádost o vydání následného certifikátu

Při vydávání následného certifikátu není vyžadována fyzická přítomnost žadatele na pracovišti registrační autority. O vydání následného certifikátu se žádá elektronickou cestou. Žadatel se autentizuje použitím zaručeného elektronického podpisu založeného na certifikátu vydaném PostSignum Public CA.

3.4 Žádost o zneplatnění certifikátu

Žadatel nebo držitel certifikátu se při žádosti o zneplatnění certifikátu autentizuje

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

V certifikační politice může být definováno, že o zneplatnění certifikátu mají právo žádat i jiné osoby než držitel certifikátu. V tomto případě je v politice stanoveno rovněž to, jakým způsobem se tato osoba při žádosti o zneplatnění certifikátu identifikuje a autentizuje.

4. PROVOZNÍ POŽADAVKY

4.1 Registrace žádosti o certifikát

Postupy registrace žádosti o certifikát jsou definovány v jednotlivých certifikačních politikách.

4.1.1 Žadatelé o certifikát

PostSignum VCA je orientována na:

- Zákazníky - organizace, které chtějí vydat certifikáty pro zaměstnance, kteří mají k organizaci určitý vztah. Proces žádosti o certifikát je několikastupňový a až v konečné fázi

přichází žadatel o certifikát k registrační autoritě s elektronickou žádostí o certifikát a s příslušnými doklady.

- Zákazníky - fyzické osoby, které si chtějí nechat vydat certifikáty. Proces žádosti o certifikát je jednostupňový, v rámci jedné návštěvy registrační autority zákazník naváže smluvní vztah a proběhne i vydání certifikátu na základě přinesené elektronické žádosti o certifikát.

4.1.2 Uzavření smlouvy se zákazníkem - organizací

Postup a požadavky na uzavření smlouvy se zákazníkem - organizací jsou popsány v příslušné certifikační politice.

4.1.3 Uzavření smlouvy se zákazníkem - fyzickou osobou

Postup a požadavky na uzavření smlouvy se zákazníkem - fyzickou osobou jsou popsány v příslušné certifikační politice.

4.2 Zpracování žádostí o certifikát

Vydání certifikátu může ve vybraných případech následovat ihned po podpisu smlouvy na registrační autoritě.

4.2.1 Kontrola oprávněnosti žádosti - organizace

Postup a požadavky na kontrolu oprávněnosti žádosti jsou popsány v příslušné certifikační politice.

4.2.2 Kontrola oprávněnosti žádosti - fyzická osoba

Postup a požadavky na kontrolu oprávněnosti žádosti jsou popsány v příslušné certifikační politice.

4.3 Vydání certifikátu

Postup a požadavky na vydání certifikátu jsou popsány v příslušné certifikační politice. Obecně však platí, že

- 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;

- od okamžiku rozhodnutí je poskytovatel povinen vydat certifikát do následujícího pracovního dne;

- vydaný certifikát, u kterého byl vysloven souhlas se zveřejněním, je do 24 hodin od převzetí certifikátu žadatelem zveřejněn na webových stránkách PostSignum VCA.

4.4 Převzetí certifikátu

Postup a požadavky na převzetí certifikátu jsou popsány v příslušné certifikační politice.

4.4.1 Komunikace poskytovatele certifikačních služeb se zákazníkem

Certifikát je typicky vydán žadateli krátce po schválení žádosti a jejím vložení do systému certifikační autority. V tomto případě převezme žadatel vydaný certifikát osobně na pracovišti registrační autority. Pokud dojde vinou poskytovatele certifikačních služeb ke zdržení vydání certifikátu, domluví se pracovník registrační autority nebo příslušného obchodního místa se žadatelem nebo oprávněnou osobou na způsobu náhradního převzetí certifikátu.

4.4.2 Zveřejnění vydaného certifikátu poskytovatelem

Certifikát, u kterého byl držitelem vysloven souhlas se zveřejněním, je do 24 hodin od převzetí zveřejněn v adresářových službách PostSignum VCA a na webových stránkách PostSignum VCA.

4.4.3 Oznámení o vydání certifikátu ostatním uživatelům

Kromě zveřejnění vydaného certifikátu, u kterého byl držitelem vysloven souhlas se zveřejněním, neoznamuje poskytovatel certifikačních služeb vydání certifikátu žádné třetí straně.

4.5 Použití klíče a certifikátu

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

4.5.1 Užití soukromého klíče a certifikátu držitelem

Držitel certifikátu vydaného PostSignum VCA je oprávněn používat soukromý klíč a odpovídající certifikát pouze pro účely specifikované v certifikační politice, podle které byl daný certifikát vydán.

4.5.2 Užití veřejného klíče a certifikátu spoléhající se stranou

Spoléhající se strana je oprávněna použít certifikát vydaný PostSignum VCA pouze pro účely specifikované v certifikační politice, podle které byl daný certifikát vydán.

4.6 Obnova certifikátu

Certifikační autorita PostSignum VCA neprovádí obnovu certifikátů se stejným klíčovým párem. O obnově certifikátu s novým klíčovým párem - vydání následného certifikátu - pojednává kapitola 4.7.

4.7 Vydání následného certifikátu

Vydání následného certifikátu probíhá způsobem definovaným certifikační politikou. Obecně platí, že žádost o vydání následného certifikátu je zaslána emailovou zásilkou podepsanou zaručeným elektronickým podpisem na vyhrazenou registrační autoritu a vydaný certifikát je poté dostupný na webových stránkách, kde je prováděna jeho akceptace a stažení.

4.8 Změny údajů v certifikátu

Dojde-li ke změně údajů v certifikátu vydaného PostSignum VCA, musí držitel certifikátu tuto změnu neprodleně ohlásit poskytovateli certifikačních služeb. Za zákazníka - organizaci

oznamuje změny v certifikátech zaměstnanců oprávněná osoba, a to buď telefonicky nebo písemně. K oznámení změn využije kontaktní údaje uvedené ve smlouvě o poskytování certifikačních služeb. Fyzická osoba oznamuje změny údajů v certifikátech osobně na pracovišti registrační autority, telefonicky nebo písemně.

Poskytovatel certifikačních služeb rozhodne, zda je třeba vydaný certifikát zneplatnit, a učiní potřebné kroky. Vydání certifikátu s novými údaji probíhá stejně jako vydání prvního certifikátu.

4.9 Zneplatnění certifikátu

4.9.1 Důvody zneplatnění certifikátu

Důvody pro zneplatnění certifikátu koncového uživatele jsou především následující:

- jakékoliv podezření na kompromitaci odpovídajícího soukromého klíče,
- neplnění podmínek smlouvy o poskytování certifikačních služeb ze strany zákazníka,
- příslušná žádost držitele nebo žadatele,
- další důvody (úmrtí, zánik, zbavení nebo omezení právní způsobilosti žadatele; pozbytí pravdivosti údajů, na jejichž základě byl certifikát vydán).

Obecně se jedná o případy, kdy existuje riziko zneužití vydaného a platného certifikátu.

4.9.2 Osoby oprávněné žádat o zneplatnění certifikátu

O zneplatnění certifikátu může požádat jak žadatel, tak i zákazník (držitel certifikátu).

Zneplatnění certifikátu může iniciovat manažer VCA jakožto zástupce certifikační autority, která vydala certifikát.

4.9.3 Postup zneplatnění certifikátu na žádost zákazníka - organizace

Postup a požadavky na zneplatnění certifikátu jsou popsány v příslušné certifikační politice.

4.9.4 Postup zneplatnění certifikátu na žádost zákazníka - fyzické osoby

Postup zneplatnění certifikátu pro zákazníka, který je fyzickou osobou, je shodný s postupy pro zneplatnění na žádost žadatele.

4.9.5 Postup zneplatnění pro žadatele

Postup a požadavky na zneplatnění certifikátu na žádost žadatele jsou popsány v příslušné certifikační politice.

4.9.6 Zneplatnění certifikátu z vůle certifikační autority

Postup a požadavky na zneplatnění certifikátu z vůle certifikační autority jsou popsány v příslušné certifikační politice.

4.9.7 Časová prodleva od přijetí žádosti o zneplatnění

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

4.9.8 Možnosti ověření stavu certifikátu

Stav certifikátu je možné ověřit na aktuálním CRL zveřejněném v adresářových službách nebo na webových stránkách PostSignum VCA.

4.9.10 Zveřejňování seznamu zneplatněných certifikátů (CRL)

Seznam zneplatněných certifikátů a informace o stavu certifikátu jsou považovány za veřejně přístupné informace. V seznamu zneplatněných certifikátů je jako nepovinná rozšiřující položka uveden důvod revokace certifikátu ve formátu podporovaném standardem X.509.

Seznam zneplatněných certifikátů (CRL) je zveřejňován na třech místech:

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

Primárním zdrojem aktuálního CRL jsou webové stránky PostSignum VCA.

Seznam zneplatněných certifikátů (CRL) kořenové certifikační autority PostSignum Root QCA je zveřejňován alespoň jedenkrát ročně.

Seznam zneplatněných certifikátů (CRL) podřízených certifikačních autorit v hierarchii PostSignum VCA je zveřejňován alespoň každých 12 hodin.

4.9.11 Platnost CRL

CRL kořenové certifikační autority PostSignum Root QCA je platný jeden rok od vydání.

CRL podřízených certifikačních autorit v hierarchii PostSignum VCA je platný 12 hodin.

4.9.12 Možnosti on-line ověření stavu certifikátu

Stav certifikátu je možné ověřit pouze na aktuálním CRL.

PostSignum VCA neposkytuje informace o stavu certifikátu protokolem OCSP.

4.9.13 Další možnosti ověření stavu certifikátu

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

4.9.14 Kompromitace soukromého klíče držitele certifikátu

Jakékoliv podezření na kompromitaci soukromého klíče držitele certifikátu je tento povinen neprodleně prověřit a výsledek oznámit poskytovateli certifikačních služeb, který učiní kroky potřebné ke zneplatnění odpovídajícího certifikátu.

4.9.15 Pozastavení platnosti certifikátu

Certifikátu vydanému certifikační autoritou PostSignum VCA není možné pozastavit platnost. Certifikáty je možné pouze zneplatňovat.

4.10 Zjišťování stavu certifikátu

4.10.1 Charakteristika služby

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 není závazná, jedná se pouze o doplňkovou informaci k aktuálnímu CRL, které je zdrojem informací o stavu certifikátu.

4.10.2 Dostupnost služby

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

4.11 Konec platnosti certifikátu

Možné případy ukončení platnosti certifikátu jsou uvedeny v příslušné certifikační politice.

4.12 Úložiště a obnova soukromých klíčů držitelů certifikátů

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

5. BEZPEČNOST FYZICKÁ, PROCEDURÁLNÍ A PERSONÁLNÍ

Pro PostSignum VCA byl zpracovány dokumenty:

- Systémová bezpečnostní politika, popisující zásady bezpečnosti v oblasti fyzické, procedurální a personální,

- Provozní a bezpečnostní procedury, popisující na logické úrovni postupy dodržované v PostSignum VCA.

Oba 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 Oblast fyzické bezpečnosti

5.1.1 Umístění a architektura

V PostSignum VCA existují tři typy pracovišť:

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

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 Zdroj elektřiny, klimatizace

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

5.1.4 Ohrožení vodou

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 prevence a zabezpečení

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 Uskladnění nosičů dat

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

5.1.7 Nakládání s odpady; likvidace

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

- magnetická 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 Záložní lokalita

Pro PostSignum VCA byla vybudována záložní lokalita, kam provoz přechází v mimořádných situacích, kdy není možné zabezpečit řádný provoz VCA v hlavní lokalitě.

5.2 Procedurální bezpečnost

5.2.1 Určení rolí

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.

5.2.2 Nezbytné počty osob pro činnosti

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 (nástrojem pro vytváření elektronického podpisu) certifikační autority.

5.2.3 Identifikace a autentizace pro každou roli

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

3.2.4 Oddělení pravomocí

V PostSignum VCA jsou stanovena pravidla, podle kterých jsou obsazovány jednotlivé role a rovněž byla stanovena pravidla pro separaci rolí.

5.3 Personální bezpečnost

5.3.1 Požadavky na osobnostní profil, kvalifikaci a praxi v oboru

Funkce, 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.

5.3.2 Zkoumání důvěryhodnosti

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.

5.3.3 Požadavky na školení a další vzdělávání

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.

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

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

5.3.4 Požadavky na proškolování a jeho frekvence

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 Požadavky na rotaci pracovníků a její frekvenci

Požadavky na rotaci pracovníků a její frekvenci nejsou definovány.

5.3.6 Postihy za porušení pracovní kázně

Postihy za porušení pracovní kázně se řídí organizačními předpisy České pošty, s.p.

5.3.7 Požadavky na smluvní pracovníky

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

5.3.8 Dokumentace poskytovaná personálu

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

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

5.4 Procedury kontroly bezpečnostní shody

Pro PostSignum VCA byl zpracován dokument Auditní a archivační politika (je přílohou bezpečnostní politiky), 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.

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

5.4.2 Zpracovávání auditních záznamů

Auditní záznamy jsou kontrolovány osobami v odpovídající roli pověřené tímto úkolem. Dále podléhají interní a externí kontrole.

5.4.3 Doba uchovávání 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 uchovávány na nepřepisovatelných médiích.

5.4.5 Uchovávání auditních záznamů

Po uplynutí archivační doby jsou záznamy skartovány podle předpisů platných v České poště, s.p. s tím, že každé takové skartování je předem písemně schváleno manažerem VCA.

Za auditní záznamy jsou považovány i veškeré písemné protokoly a smlouvy související s registrací žádosti o certifikát.

5.4.6 Procedury kontroly

Procedury interní kontroly se řídí interními předpisy České pošty. Procedury externí kontroly se řídí smlouvou externího auditora s Českou poštou.

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

5.4.7 Zprávy o mimořádných událostech

O mimořádných událostech (bezpečnostních incidentech atd.) v PostSignum VCA jsou vedeny záznamy a vypracovávány zprávy podle [PBIT]. Tyto zprávy jsou mimo šíření podle [PBIT] předávány i Auditorovi VCA.

5.4.8 Hodnocení zranitelnosti

Pro PostSignum VCA byla provedena analýza rizik vedoucí k návrhu bezpečnostní politiky systému a k implementaci bezpečnostních opatření minimalizujících možnost úspěšného útoku na PostSignum VCA.

5.5 Archivace záznamů

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 uchovávaných archivních záznamů

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 archivace

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

5.5.3 Zabezpečení archivu

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

5.5.4 Zálohovací procedury archivu

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 časová razítka pro záznamy

V PostSignum VCA se nepoužívají časová razítka.

5.5.6 Postupy zpřístupnění a ověřování archivovaných záznamů.

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 klíčů certifikační autority

Platnost klíčů certifikační autority PostSignum VCA je omezena. Nejméně 14 dní před vypršením platnosti certifikátu je provozovatel certifikační autority povinen požádat o vydání dalšího certifikátu u PostSignum Root QCA.

Plánovaná výměna klíčů certifikační autority musí být oznámena zákazníkům nejpozději tři měsíce před uskutečněním výměny. Toto oznámení bude (včetně důvodu ukončení platnosti certifikátu) zveřejněno na webových stránkách PostSignum VCA a na všech pracovištích registrační autority PostSignum VCA.

5.7 Činnost po kompromitaci a obnova po mimořádné události

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 Zabezpečení prostředků certifikační autority po živelné katastrofě nebo jiné mimořádné události

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

5.7.2 Poškození výpočetních zdrojů, software a/nebo dat

Zabezpečení výpočetních zdrojů, software a dat certifikační autority po živelné katastrofě nebo jiné mimořádné události je rozpracováno v dokumentu Krizový plán ochrany objektu.

5.7.3 Kompromitace soukromého klíče certifikační autority PostSignum VCA

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

PostSignum Root QCA okamžitě zneplatní certifikát certifikační autority PostSignum VCA, zneplatněný certifikát bude nejpozději do 12 hodin zveřejněn na CRL PostSignum Root QCA.

Po zveřejnění informace o mimořádném ukončení činnosti končí platnost všech certifikátů vydaných certifikační autoritou PostSignum VCA.

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

5.7.4 Podezření na kompromitaci soukromého klíče PostSignum Root QCA

Případ podezření na kompromitaci soukromého klíče PostSignum Root QCA řeší Certifikační prováděcí směrnice PostSignum QCA.

5.7.5 Pokračování obchodních procesů po havárii

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

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

5.8 Ukončení činnosti kořenové certifikační autority

Ukončení činnosti PostSignum Root QCA řeší Certifikační prováděcí směrnice PostSignum QCA.

5.9 Ukončení činnosti PostSignum VCA

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

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

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

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

ČP prokazatelně zničí data pro vytváření elektronického podpisu certifikační autority PostSignum VCA, která sloužila pro podepisování certifikátů a seznamů zneplatněných certifikátů.

5.10 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.

5.11 Ukončení činnosti poskytovatele certifikačních služeb

Poskytovatel je povinen informovat každého držitele v dostatečném předstihu o svém záměru ukončit svou činnost. Poskytovatel se především zavazuje v případě ukončení poskytování certifikačních služeb:

- informovat všechny dotčené strany,

- ukončit poskytování certifikačních služeb,

- uchovat veškeré údaje spojené s činností poskytovatele dle příslušné certifikační politiky po dobu nejméně 10 let,

- prokazatelně zničit párová data pro vytváření elektronických podpisů certifikační autority PostSignum VCA.

6. TECHNICKÁ BEZPEČNOST

6.1 Generování párových dat a jejich instalace

6.1.1 Generování párových dat pro žadatele o certifikát

PostSignum VCA neposkytuje funkci generování párových dat pro žadatele o certifikát.

Klíče žadatelů o certifikát mohou být generovány jak v hardware, tak v software.

6.1.2 Doručení soukromého klíče žadateli o certifikát

Protože PostSignum VCA neposkytuje funkci generování párových dat pro žadatele o certifikát, nebyly definovány postupy pro předání soukromého klíče žadateli.

6.1.3 Doručení veřejného klíče poskytovateli certifikačních služeb

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

6.1.4 Distribuce veřejného klíče poskytovatele certifikačních služeb klientům

Veřejný klíč poskytovatele certifikačních služeb je klientům předán spolu s jejich vlastním právě vydaným certifikátem prostřednictvím pracoviště registrační autority.

6.1.5 Velikost klíčů/modulů

Délky používaných klíčů/modulů jsou stanoveny v příslušných certifikačních politikách.

Klíče certifikační autority PostSignum VCA mají pro algoritmus RSA délku 2048 bitů. Klíče držitelů certifikátů mají pro algoritmus RSA délku 1024 a 2048 bitů.

6.1.6 Generování parametrů veřejného klíče a testování kvality parametrů

Parametry používané při vytváření veřejných klíčů komponent PostSignum VCA jsou generovány odpovídajícím softwarovým vybavením (UniCERT). Použité algoritmy a jejich parametry odpovídají vyhlášce [V366] resp. její příloze.

Parametry používané při vytváření veřejných klíčů žadatelů o certifikát jsou generovány softwarovým vybavením žadatele a poskytovatel certifikačních služeb za ně nenese 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 Hardwarové/softwarové generování klíčů certifikačních autorit a obsluhy PKI

Klíče certifikační autority jsou generovány v odpovídajícím hardwarovém modulu, klíče obsluhy jsou generovány v čipových kartách.

6.1.8 Užití klíče

Klíče koncových uživatelů mohou být použity pouze v souladu s pravidly popsanými v kapitole 1.5.

6.2 Ochrana soukromého klíče poskytovatele (dat pro vytváření elektronických podpisů poskytovatele)

6.2.1 Standardy/normy pro kryptografický modul

Kryptografický modul použitý pro generování a úschovu soukromého klíče certifikační autority (nástroj pro vytváření elektronického podpisu) PostSignum VCA splňuje požadavky standardu FIPS 140-1 Level 4.

6.2.2 Operace se soukromým klíčem

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

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

6.2.3 Možnost obnovy soukromého klíče

Soukromý klíč certifikační autority může být obnoven ze záloh, avšak je k tomu zapotřebí minimálně dvou osob.

6.2.4 Záloha soukromého klíče

Soukromý klíč certifikační autority je zálohován za součinnosti několika osob, minimálně však tří osob.

Soukromý klíč je zálohován na čipové karty v zašifrované podobě. Klíč použitý pro šifrování je exportován na čipové karty takovým způsobem, že k jeho obnově je třeba dvou z těchto karet. Čipové karty jsou ukládány tak, že pro přístup ke třem kartám (jedna karta se zašifrovanou zálohou soukromého klíče, dvě karty s exportním klíčem) nezbytným pro obnovu soukromého klíče je třeba součinnosti alespoň dvou osob, každé s jinou rolí.

6.2.5 Archivace soukromého klíče

Soukromé klíče certifikační autority PostSignum VCA nejsou archivovány. Po ukončení provozu certifikační autority jsou protokolárně zničeny.

6.2.6 Vkládání soukromého klíče do kryptografického modulu

Soukromý klíč certifikační autority je generován v kryptografickém modulu (nástroji pro vytváření elektronického podpisu) 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 se Systémovou bezpečnostní politikou, Provozními a bezpečnostními procedurami a Auditní a archivační politikou.

Klíč je do kryptografického modulu vkládán z čipové karty po autentizaci dvou pracovníků obsluhy, kteří nemohou získat přístup ke kartě se zálohou soukromého klíče. Pokud je klíč vkládán do kryptografického modulu, ze kterého nebyl exportován, nebo byl modul mezi exportem a vložením klíče deaktivován, musí být vložen také klíč použitý pro šifrování soukromého klíče z dalších dvou čipových karet.

6.2.7 Způsob aktivace soukromého klíče

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

6.2.8 Způsob deaktivace soukromého klíče

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

6.2.9 Způsob 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.

Před přemístěním ze zabezpečených prostor Centrálních pracovišť je HSM uveden do inicializovaného stavu, tj. je pomocí mechanismů HSM bezpečně vymazán veškerý kryptografický materiál (včetně soukromého klíče CA).

6.2.10 Hodnocení bezpečnosti kryptografického modulu

Vzhledem k tomu, že kryptografický modul užívaný k úschově soukromého klíče certifikační autority byl vyhodnocen podle standardu FIPS 140-1 Level 4, nepředpokládá se, že by obsahoval závažné chyby na úrovni designu zařízení. Přesto se průběžně sleduje, zda nebyl objeven útok na toto zařízení tak, aby bylo možné včas na takové ohrožení reagovat.

6.3 Další požadavky na správu klíčů

6.3.1 Archivace veřejného klíče

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

6.3.2 Doba, na kterou se vydávají certifikáty veřejných klíčů koncových uživatelů

Doba, na kterou se vydávají certifikáty veřejných klíčů koncových uživatelů, je stanovena v odpovídajících certifikačních politikách.

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.

6.5 Počítačová bezpečnost

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Pro každou komponentu PostSignum VCA jsou definována nastavení zajišťující bezpečnost dané komponenty na technologické úrovni.

6.5.2 Hodnocení počítačové bezpečnosti

Systém PostSignum VCA prošel externí kontrolou bezpečnostní shody.

6.6 Technické kontroly a doba životnosti

6.6.1 Dohled nad používaným IS

Nad informačním systémem PostSignum VCA je prováděn nepřetržitý dohled.

6.6.2 Dozor nad interními bezpečnostními audity (logy)

Za dozor nad interními bezpečnostními logy odpovídá bezpečnostní administrátor VCA, dozor je prováděn v souladu se Systémovou bezpečnostní politikou.

6.6.3 Hodnocení životnosti prvků

Pro kritické komponenty systému (například hardware a software PostSignum Public CA) se pravidelně vyhodnocuje, zda nehrozí jejich fyzické či morální zastarání a podle potřeby se provádí jejich obměna tak, aby byl systém nadále životaschopný a udržovatelný.

6.7 Bezpečnost počítačové sítě

Bezpečnostní parametry počítačové sítě jsou nastaveny v souladu s návrhem systému, který zohledňuje známé bezpečnostní hrozby.

6.8 Požadavky na časová razítka

PostSignum VCA nenabízí službu časových razítek.

7. PROFIL CERTIFIKÁTU A CRL

7.1 Profil certifikátu

PostSignum VCA vydává certifikáty podle standardu X.509 verze 3, v němž jsou mimo jiné definovány rozšiřující položky certifikátu, které mohou omezit použití certifikátu případně poskytovat dodatečné informace o certifikátu nebo jeho držiteli. PostSignum VCA podporuje rozšiřující položky popsané v odpovídajících certifikačních politikách.

7.1.1 Číslo verze(í)

PostSignum VCA vydává certifikáty vyhovující standardu X.509 Verze 3.

7.1.2 Rozšíření (extenze) certifikátu

V certifikátech se používají rozšíření specifikovaná v jednotlivých certifikačních politikách.

7.1.3 Identifikátory algoritmů

Algoritmům používaným v PostSignum VCA nejsou přiřazeny OID. V certifikační autoritě PostSignum VCA se nepoužívají specifické algoritmy, které by vyvíjel provozovatel PostSignum VCA nebo jeho dodavatel, ale pouze algoritmy odpovídající vyhlášce [V366] resp. její příloze.

7.1.4 Použitá jména

Certifikáty vydávané PostSignum VCA obsahují obchodní firmu a IČ vystavitele certifikátu a obchodní firmu nebo název nebo jméno a příjmení držitele certifikátu.

7.1.5 Omezení platná u použitých jmen

Použitá jména musí být přesnou transkripcí nebo přesnou transkripcí bez diakritiky zákazníka žádajícího o vydání certifikátu.

Další pravidla pro vytváření jmen a případná další omezení jsou uvedena v příslušné certifikační politice.

7.1.6 Identifikátor certifikační politiky

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

7.1.7 Rozšiřující položka „Policy Constraints“

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

7.1.8 Rozšiřující položka „Policy Qualifier“

Rozšiřující položka „Policy Qualifier“ se v PostSignum VCA používá. Obsahuje odkaz na webové stránky PostSignum VCA, kde lze získat certifikační politiku, podle které byl certifikát vydán, a odpovídající CPS.

7.2 Profil seznamů certifikátů, které byly zneplatněny (CRL)

7.2.1 Čísla verzí dle X.509

V PostSignum VCA jsou vydávány seznamy zneplatněných certifikátů podle standardu X.509 Verze 2.

7.2.2 Rozšíření standardního CRL

V seznamech zneplatněných certifikátů se používají následující rozšiřující položky:

- Authority Key Identifier,
  - KeyIdentifier,
  - AuthorityCertIssuer, AuthorityCertSerialNumber,
- CRL Number,
- Revocation Reason,
- Invalidity Date (volitelně).

7.3 OCSP

PostSignum VCA neposkytuje informace o stavu certifikátu protokolem OCSP.

8. HODNOCENÍ SHODY A SOULADU S PŘEDPISY (AUDIT)

8.1 Periodicita provádění auditu

Pravidelně jsou prováděny interní kontroly (jednou za 12 měsíců) a dílčí kontroly (jednou za 3 měsíce). Externí kontroly jsou prováděny jednou za 4 roky. Tyto pravidelné audity a kontroly mohou být podle potřeby doplněny další kontrolou, mimo jiné na základě rozhodnutí manažera VCA, managementu České pošty nebo odboru interního auditu České pošty, resp. odboru kontroly České pošty.

8.1.1 Dílčí kontrola

Každé čtvrtletí je pracovníky, kteří se nepodílí na provozu PostSignum VCA, ověřeno dodržování obecně závazných a interních předpisů, bezpečnost a integrita systémů PostSignum VCA. (Tito pracovníci jsou označováni v dokumentaci VCA jako Auditoři VCA.)

O provedení každé kontroly musí být vypracována podepsaná písemná zpráva. Tato zpráva je archivována stejným způsobem jako ostatní záznamy o provozu PostSignum VCA a uchovávána nejméně po dobu deseti let.

8.1.2 Interní kontrola

Nejméně jednou za dvanáct měsíců je pracovníky odboru interního auditu pro PostSignum VCA:

- ověřeno dodržování obecně závazných právních předpisů, vnitřních předpisů, přijatých opatření a stanovených postupů,
- ověřena přiměřenost, funkčnost, účinnost a efektivnost řízení rizik, vnitřních řídicích a kontrolních systémů a mechanismů.

O provedení každé kontroly musí být vypracována podepsaná písemná zpráva. Tato zpráva je archivována stejným způsobem jako ostatní záznamy o provozu PostSignum VCA a uchovávána nejméně po dobu deseti let.

8.1.3 Externí kontrola

Nejméně jednou za 4 roky je bezpečnost a integrita systémů a procesů PostSignum VCA ověřena externí kontrolou provedenou auditorem nezávislým na České poště.

O provedení každé kontroly musí být vypracována podepsaná písemná zpráva. Tato zpráva je archivována stejným způsobem jako ostatní záznamy o provozu PostSignum VCA a uchovávána nejméně po dobu deseti let.

8.2 Identita a kvalifikace auditora

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 Auditoři VCA.

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

8.3 Vztah auditora k poskytovateli certifikačních služeb

Kontrolu provádí zaměstnanci České pošty, s.p.

Interní kontrolu provádí zaměstnanci České pošty, s.p.

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

8.4 Oblasti kontroly

V rámci kontrol je ověřováno dodržování obecně závazných a interních předpisů, bezpečnost a integrita systémů.

V rámci pravidelné interní kontroly je hodnoceno dodržování obecně závazných právních předpisů, vnitřních předpisů, přijatých opatření a stanovených postupů, a přiměřenost, funkčnost, účinnost a efektivnost řízení rizik, vnitřních řídicích a kontrolních systémů a mechanismů.

V rámci externí kontroly se hodnotí zejména bezpečnost a integrita systémů a procesů VCA.

8.5 Opatření v případě zjištění nedostatků

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

8.6 Distribuce (rozdělovník) a projednání výsledku kontroly

O provedení každé kontroly je vypracována podepsaná písemná zpráva. Tato zpráva je archivována stejným způsobem jako ostatní záznamy o provozu PostSignum VCA a uchovávána nejméně po dobu deseti let.

Výsledky kontroly jsou považovány za obchodní tajemství (OBT). Výsledky jsou předávány manažerovi VCA. Ten zajistí jejich distribuci a projednání. Pokud je součástí výsledků samostatný výrok auditora, může manažer VCA rozhodnout o jeho zveřejnění.

9. DALŠÍ OBCHODNÍ A PRÁVNÍ ZÁSADY

9.1 Poplatky za služby

9.1.1 Poplatky za vydání certifikátu

Cena za vydání certifikátu je stanovena v ceníku služeb České pošty, s.p.

9.1.2 Poplatky za zneplatnění nebo informaci o stavu certifikátu

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

9.1.3 Náhrady za škody

Náhrady za škody jsou stanoveny v odpovídající certifikační politice.

9.2 Finanční odpovědnost

9.2.1 Finanční krytí odpovědnosti poskytovatele certifikačních služeb

Finanční krytí je uvedeno v odpovídající certifikační politice.

9.3 Zásady ochrany informací (utajení)

Ochrana informací v prostředí PostSignum VCA se řídí bezpečnostními politikami závaznými pro PostSignum VCA. Tento dokument je přístupný všem osobám s přístupem k systému PostSignum VCA a rovněž osobám, které provádějí kontrolu.

9.3.1 Specifikace utajovaných informací

Definice informací, jejichž důvěrnost musí být zaručena, je uvedena v příslušné certifikační politice.

9.3.2 Informace nepovažované za důvěrné

Definice informací, které nejsou považovány za důvěrné, je uvedena v příslušné certifikační politice.

9.3.3 Zodpovědnost za ochranu důvěrných informací

Odpovědnost za zpracování důvěrných informací v úloze PostSignum VCA nese Česká pošta, jakožto poskytovatel certifikačních služeb.

9.4 Ochrana osobních údajů

9.4.1 Plán ochrany osobních údajů

ČP provedla analýzu bezpečnostních rizik a na jejím základě stanovila opatření na ochranu zpracovávaných osobních údajů. Podrobná specifikace přijatých bezpečnostních opatření je obsažena v interních dokumentech ČP. Tyto dokumenty jsou pravidelně předmětem kontroly bezpečnostní shody. V příslušné certifikační politice a částečně i v tomto dokumentu jsou popsána základní bezpečnostní opatření. ČP průběžně sleduje bezpečnostní prostředí v obdobných společnostech v Evropě s cílem reagovat na potenciální nová bezpečnostní rizika.

9.5 Ochrana duševního vlastnictví

Certifikační politiky, certifikační prováděcí směrnice a veškeré související dokumenty jsou chráněny autorskými právy České pošty a představují významné know-how České pošty. Česká pošta je rovněž nositelem práv k informačnímu systému pro provoz certifikační autority a ke struktuře, organizaci, vzhledům obrazovek a obsahu webových stránek PostSignum VCA. ČP je nositelem následujících registrací doménových jmen, souvisejících s poskytováním certifikační autority: postsignum.cz.

9.6 Záruky ČP

Záruky České pošty jsou uvedené v příslušné certifikační politice.

9.7 Omezení záruk

Příslušná ujednání o omezení záruk jsou uvedená v příslušné certifikační politice.

9.8 Omezení odpovědnosti

Ujednání o omezení odpovědnosti je uvedeno v příslušné certifikační politice.

9.9 Náhrada škody

Finanční krytí odpovědnosti poskytovatele certifikačních služeb vůči zákazníkům a spoléhajícím se stranám je popsáno v kapitole 9.2.

9.10 Platnost dokumentu a ukončení platnosti

Platnost dokumentu je ošetřena v kapitole 1.6.

9.11 Obecné zásady

9.11.1 Povinnosti

9.11.1.1 Povinnosti PostSignum Root QCA

Povinnosti PostSignum Root QCA jsou stanoveny v dokumentu Certifikační prováděcí směrnice PostSignum QCA aktuální verze.

9.11.1.2 Povinnosti PostSignum Public CA

Certifikační autorita PostSignum Public CA má zejména tyto povinnosti:

- věnovat náležitou péči všem činnostem spojeným s poskytováním certifikačních služeb; náležitá péče zahrnuje provoz v souladu
  - s provozní dokumentací,
  - příslušnou certifikační politikou,
  - touto certifikační prováděcí směrnicí,
  - systémovou bezpečnostní politikou,

  - platnými právními předpisy,

- schválit zřízení registrační autority, která bude spadat do její působnosti,

- ve sféře své působnosti vynucovat dodržování pravidel popsaných v této certifikační prováděcí směrnici,

- zveřejňovat certifikační politiky, podle kterých vydává certifikáty, na webových stránkách PostSignum VCA, případně jinými vhodnými způsoby,

- bez zbytečných odkladů posoudit žádost o certifikát, vydat rozhodnutí, zda bude certifikát vydán, a o tomto rozhodnutí informovat žadatele,

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

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

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

- zveřejnit certifikát u kterého byl vysloven souhlas se zveřejněním a který byl akceptován žadatelem, bez zbytečných odkladů v adresářových službách PostSignum VCA, na webových stránkách PostSignum VCA, případně jiným vhodným způsobem,

- revokovat certifikát podle pravidel popsaných v certifikační politice,

- informovat držitele certifikátu o tom, že jeho certifikát byl revokován z vůle certifikační autority,

- zveřejnit seznam zneplatněných certifikátů bez zbytečného prodlení, ve lhůtě uvedené v certifikační politice,

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

- asistovat při kontrole, který provádí externí auditor nebo pověřený pracovník České pošty.

9.11.1.3 Povinnosti registrační autority

Registrační autorita má zejména tyto povinnosti:

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

  - se smlouvou mezi Českou poštou, s.p. a danou registrační autoritou, pokud jsou provozovatelé certifikační autority a registrační autority různé právní subjekty,

  - s provozní dokumentací,

  - příslušnou certifikační politikou,

  - touto certifikační prováděcí směrnicí,
  - systémovou bezpečnostní politikou,
  - platnými právními předpisy,
- ve sféře své působnosti vynucovat dodržování pravidel popsaných v této certifikační prováděcí směrnici,
- přijímat žádosti o certifikát včetně odpovídajících písemných dokladů, schvalovat žádosti nebo je zamítat podle pravidel daných příslušnou certifikační politikou,
- poučit žadatele o jeho povinnostech vyplývajících z příslušné certifikační politiky, poskytnout žadateli tuto certifikační politiku nebo informaci, kde lze certifikační politiku získat,
- postoupit ke zpracování žádost obsahující věcně správné údaje s ohledem na informace, které má registrační autorita k dispozici v okamžiku přijetí žádosti, a bez chyb vzniklých při zadávání údajů obsluhou registrační autority,
- postoupit ke zpracování žádost o certifikát odpovídající standardu X.509 a splňující náležitosti vyžadované příslušnou certifikační politikou,
- ověřovat totožnost žadatele o certifikát v souladu s příslušnou certifikační politikou,
- bez zbytečných odkladů posoudit žádost o certifikát, vydat rozhodnutí, zda bude certifikát vydán, a o tomto rozhodnutí informovat žadatele,
- informovat žadatele o tom, že certifikát byl vydán, a předat respektive zajistit předání vydaného certifikátu žadateli,
- revokovat certifikát podle pravidel popsaných v certifikační politice,
- prověřit podezření, že došlo k prozrazení soukromého klíče v rámci působnosti dané registrační autority, což by mohlo vést ke ztrátě důvěryhodnosti dané registrační autority,
- pořizovat evidenci dokladů spojených s přijetím a zpracováním žádosti a vydáním certifikátu,
- asistovat při kontrole, který provádí externí auditor nebo pověřený pracovník České pošty.

9.11.1.4 Povinnosti zákazníků a žadatelů o certifikát

Povinnosti zákazníků a žadatelů o certifikát jsou stanoveny v příslušných certifikačních politikách.

9.11.1.5 Povinnosti spoléhajících se stran a ostatních uživatelů

Uživatel certifikátu vydaného PostSignum Public CA musí zejména:

- Získat certifikáty PostSignum Root QCA a PostSignum Public CA z bezpečného zdroje (webové stránky PostSignum VCA) a ověřit otisk („fingerprint“) těchto certifikátů.

- Před použitím certifikátu vydaného certifikační autoritou PostSignum Public CA ověřit platnost certifikátu této autority a následně i platnost vydaného koncového certifikátu; kontrola se provádí na správnost podpisu vydávající autority a vůči příslušnému aktuálnímu CRL.

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

9.11.2 Odpovědnost

Provozovatel PostSignum VCA implementoval řadu opatření, která mají snížit riziko ztrát způsobených úmyslnou nebo neúmyslnou chybou personálu nebo výpadkem technologií zajišťujících provoz PostSignum VCA.

Tato opatření jsou popsána v příslušné dokumentaci, zejména v Systémové bezpečnostní politice, v Plánu zvládání krizových situací a plánu obnovy a v provozní dokumentaci.

9.11.2.1 Odpovědnost poskytovatele certifikačních služeb vůči zákazníkovi

Odpovědnost poskytovatele certifikačních služeb vůči zákazníkovi je popsána ve smlouvě o poskytování certifikačních služeb uzavřené mezi Českou poštou, s.p. a zákazníkem.

9.11.2.2 Odpovědnost registrační autority

Pokud není registrační autorita provozována Českou poštou, s.p., odpovědnost registrační autority je popsána ve smlouvě mezi Českou poštou, s.p. a provozovatelem registrační autority.

9.11.2.3 Odpovědnost zákazníků a žadatelů o certifikát

Odpovědnost zákazníků a žadatelů o certifikát je popsána ve smlouvě mezi zákazníkem a Českou poštou, s.p. a v příslušných certifikačních politikách.

9.11.2.4 Odpovědnost spoléhajících se stran a ostatních uživatelů

Odpovědností uživatelů certifikátů vydaných PostSignum VCA je plnit řádně svoje povinnosti při používání certifikátů.

9.11.3 Komunikace

9.11.3.1 Komunikace s poskytovatelem certifikačních služeb

Veškeré informace, které chce poskytovatel certifikačních služeb sdělit zákazníkům, zveřejní na svých internetových stránkách a na vývěskách na pracovištích registračních autorit. Závažné informace, jako například podezření na kompromitaci klíče některé z certifikačních autorit (PostSignum Root QCA, PostSignum Public CA), sděluje poskytovatel certifikačních služeb zákazníkovi rovněž dopisem zaslaným k rukám oprávněné osoby v případě zákazníka - organizace a k rukám držitele certifikátu v případě zákazníka - fyzické osoby.

Zákazník - organizace komunikuje s poskytovatelem certifikačních služeb prostřednictvím oprávněné osoby. Oprávněná osoba se obrací na pracoviště registrační autority nebo regionálních obchodních míst.

Zákazník - fyzická osoba komunikuje s poskytovatelem certifikačních služeb prostřednictvím pracovišť registrační autority nebo regionálních obchodních míst.

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 Public CA nebo jinou autoritou, kterou Česká pošta označí za důvěryhodnou, a o akceptaci jejíhož certifikátu se se zákazníkem předem písemně dohodne formou dodatku ke smlouvě.

9.11.3.2 Komunikace v rámci systému PostSignum VCA

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

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

9.12 Administrativní postupy

9.12.1 Identifikátory objektů dle standardu X.500

Česká pošta, s.p. přiřadila dle svých interních pravidel identifikátory objektů (OID).

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 této certifikační prováděcí směrnici.

Všechny OID jsou zaznamenány

- v příslušné certifikační politice:
  - OID přiřazené PostSignum Root QCA je uvedeno v každé certifikační politice vydané v rámci PostSignum VCA,
  - OID certifikačních autorit, jež mají certifikát podepsaný PostSignum Root QCA, je uvedeno v každé certifikační politice, podle níž vydávají certifikáty,
  - OID certifikační politiky je uvedeno v odpovídající certifikační politice,
- v interních dokumentech České pošty.

9.12.2 Postupy při zapracování změn do certifikačních politik a CPS

Postupy pro zapracování změn jsou uvedeny v kapitole 1.6.

9.12.3 Zásady zveřejňování a ohlašování/oznamování

Aktuální verze certifikačních politik jsou zveřejněny na webových stránkách PostSignum VCA, případně na dalších vhodných místech.

9.12.4 Změna OID

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

9.13 Postup při rozhodování sporů

Spory mezi zákazníkem a PostSignum VCA se řeší u místně a věcně příslušného soudu.

9.14 Právní předpisy (legislativní úprava)

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.

9.14.1 Soulad se standardy

Struktura této CPS vychází z RFC 3647, Internet X.509 Public Key Infrastructure Certificate policy and Certification Practices Framework. CPS se od RFC 3647 liší pouze do té míry, která umožňuje adekvátně popsat provozní postupy praktikované PostSignum VCA.

9.15 Různé

9.15.1 Řídící dokumenty

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

- Zákon 227/2000 Sb. o elektronickém podpisu v platném znění
- Vyhláška Úřadu pro ochranu osobních údajů č. 366/2001 ze dne 3. října 2001
- RFC 2511 - Internet X.509 Certificate Request Message Format
- RFC 3739 - Internet X.509 Public Key Infrastructure: Qualified Certificates Profile
- RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- ČSN ISO/IEC TR 13335
- ČSN ISO/IEC 17799

- ETSI TS 101456 - Policy requirements for certification authorities issuing qualified certificates

- CWA 14167-1: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements

9.15.2 Zmocněnské vztahy

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.

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

9.15.3 Oddělitelnost práv

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.

9.15.4 Vyšší moc

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

10. LITERATURA

[PBIT] Směrnice č. 12/2003, Politika bezpečnosti IT České pošty

[Z101] Zákon č. 101/2000 Sb. o ochraně osobních údajů v aktuálním znění

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

[V366] Vyhláška 366/2001 Úřadu pro ochranu osobních údajů o upřesnění podmínek stanovených v §6 a §7 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu