Certifikační prováděcí směrnice pro úlohu Kvalifikovaná certifikační autorita České pošty, s.p. PostSignum QCA

Verze 4.3.1

Evidence revizí a změn

Verze	Revize dokumentu	Důvod a popis změny	Autor	Schválil
1.0	31.12.2004	První verze	PCA ČP	PAA ČP
1.25	5.4.2005	Aktualizace dokumentu	PCA ČP	PAA ČP
1.26	30.6.2005	Aktualizace dokumentu	PCA ČP	PAA ČP
1.3	30.8.2005	Aktualizace dokumentu	PCA ČP	PAA ČP
1.31	19.4.2006	Aktualizace dokumentu	PCA ČP	PAA ČP
1.4	1.9.2006	Aktualizace dokumentu	PCA ČP	PAA ČP
1.41	17.8.2007	Aktualizace dokumentu	PCA ČP	PAA ČP
1.5	1.6.2010	Aktualizace dokumentu	PCA ČP	PAA ČP
2.0	1.7.2012	Aktualizace dokumentu	PCA ČP	PAA ČP
3.0	10.1.2014	Přidání služby OCSP	PCA ČP	PAA ČP
3.1	10.2.2016	Doplnění registračního procesu	PCA ČP	PAA ČP
4.0	1. 7. 2016	Změny v souvislosti s eIDAS	PCA ČP	PAA ČP
4.1	2. 10. 2017	Změny v souvislosti s akreditací nových poskytovaných služeb dle eIDAS	PCA ČP	PAA ČP
4.1	1. 9. 2020	Revize dokumentu bez změny verze – drobné změny v odkazech na dokumenty a legislativu	PCA ČP	
4.2.0	1. 9. 2021	Přidání nového způsobu ověření prostřednictvím vzdálené identifikace a drobné změny	PCA ČP	PAA ČP
4.2.1	15. 8. 2022	Revize dokumentu beze změny	PCA ČP	
4.2.2	15. 8. 2023	Revize dokumentu beze změny	PCA ČP	
4.3.0	7. 5. 2024	Rozšíření o algoritmus ECC	PCA ČP	PAA ČP
4.3.1	15. 8. 2024	Revize dokumentu beze změny	PCA ČP	

1. ÚVOD

Tato certifikační prováděcí směrnice upravuje postupy činnosti certifikačních autorit v hierarchii PostSignum QCA související s vydáváním kvalifikovaných certifikátů pro elektronický podpis, kvalifikovaných certifikátů pro elektronickou pečeť a kvalifikovaných certifikátů pro autentizaci internetových stránek (dále jen certifikáty) podle všech platných certifikačních politik.

1.1 Přehled

Česká pošta, s. p. (dále i Česká pošta či ČP), jako poskytovatel certifikačních služeb, ustavila dvouúrovňovou hierarchii certifikačních autorit PostSignum QCA, v jejímž rámci jsou provozovány certifikační autority vydávající kvalifikované certifikáty. Kořenem této hierarchie je PostSignum Root QCA, vydávající certifikáty pro elektronickou pečeť podřízeným certifikačním autoritám. Hierarchie certifikačních autorit, tvořená PostSignum Root QCA, podřízenou certifikační autoritou PostSignum Qualified CA a případně dalšími podřízenými certifikačními autoritami, u kterých tak Česká pošta explicitně určí, se nazývá PostSignum QCA (zkráceně QCA) a slouží k vydávání kvalifikovaných certifikátů koncovým uživatelům.

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

Certifikační autorita PostSignum QCA 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 (nebo odkazy na dokumenty popisující tyto postupy),

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

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

1.1.1 Certifikační služby poskytované PostSignum QCA

Certifikační služby nabízené certifikační autoritou PostSignum QCA jsou uvedeny v příslušných certifikačních politikách.

Pro vydávání certifikátů podřízeným certifikačním autoritám v hierarchii PostSignum je vytvořena speciální politika PostSignum Root QCA.

1.2 Název a jednoznačné určení dokumentu

Název dokumentu	Certifikační prováděcí směrnice PostSignum QCA
Verze dokumentu	4.3.1
Stav	finální
OID PostSignum Root QCA	2.23.134.1.4.2.1

OID tohoto CPS	Není přidělováno
Datum vydání	7. 5. 2024
Datum účinnosti	17. 5. 2024
Datum revize	15. 8. 2024
Doba platnosti	Do odvolání nebo do dne ukončení služeb autorit PostSignum QCA.

1.3 Participující subjekty

Tato certifikační prováděcí směrnice se týká

- všech certifikačních služeb, které jsou poskytovány podřízenou certifikační autoritou z hierarchie PostSignum QCA,
- všech certifikátů, které byly vydány kteroukoliv z podřízených certifikačních autorit v této hierarchii.

1.3.1 Certifikační autority (dále „CA“)

PostSignum QCA je tvořena hierarchií certifikačních autorit. Je zastřešující institucí, v rámci které působí ostatní certifikační autority.

Služby certifikačních autorit jsou zajišťovány poskytovatelem certifikačních služeb.

Kontaktní údaje provozovatele certifikačních služeb jsou uvedeny a zveřejněny v každé certifikační politice, podle které daná certifikační autorita vydává certifikáty, a na webových stránkách poskytovatele.

1.3.1.1 PostSignum Root QCA

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 Root QCA zajišťuje zejména tyto služby (v souladu s dokumentovanými provozními postupy):

- generování vlastních klíčů,
- vydání samo podepsaného certifikátu pro elektronickou pečeť,
- zveřejnění vlastního certifikátu pro elektronickou pečeť na webových stránkách poskytovatele a dalšími vhodnými způsoby,
- poskytování informací o vydaných certifikátech,
- stanovení jmenných konvencí pro podřízené certifikační autority v souladu se standardem X.501 resp. návazným standardem X.520,
- administrativu spojenou s registrací žadatelů o certifikát,
- vydání certifikátů pro elektronickou pečeť pro podřízené certifikační autority,

- zneplatnění certifikátů podle pravidel stanovených v certifikačních politikách,

- zveřejňování seznamů zneplatněných certifikátů na webových stránkách poskytovatele

1.3.1.2 Podřízené certifikační autority

Hlavním úkolem podřízených certifikačních autorit v hierarchii PostSignum je vydávat a spravovat certifikáty pro zákazníky České pošty v souladu s definovanými certifikačními politikami.

Certifikační autority začleněné do hierarchie PostSignum, tedy PostSignum Qualified CA a případně další podřízené certifikační autority, které Česká pošta explicitně určí, zajišťují zejména tyto služby (v souladu s dokumentovanými provozními postupy):

- generování vlastního páru klíčů,

- podání žádosti o certifikát u PostSignum Root QCA,

- zveřejnění všech certifikačních politik, podle kterých vydávají certifikáty, na svých webových stránkách,

- administrativu spojenou s registrací žadatelů o certifikát,

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

- zneplatnění certifikátů podle pravidel stanovených v certifikačních politikách,

- zveřejňování vydaných certifikátů, s jejichž zveřejněním dal držitel souhlas na webových stránkách poskytovatele,

- zveřejňování seznamů zneplatněných certifikátů na webových stránkách poskytovatele.

1.3.2 Registrační autority (dále „RA“)

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

Registrační autority zajišťují služby uvedené v příslušné certifikační politice.

1.3.2.1Stacionární 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 pečetí) jsou přijímány na adrese

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: 954 303 303

E-mail: postsignum@cpost.cz

Web: https://www.postsignum.cz/

1.3.2.5 Centrální registrační autorita

Jedná se o systém, který zajišťuje vydání certifikátu u žadatelů, kteří svou totožnost prokázali prostřednictvím vzdálené identifikace.

1.3.3 Držitelé certifikátů a podepisující nebo pečetící osoby, kteří požádali o vydání certifikátu, a kterým byl certifikát vydán.

1.3.3.1 Zákazníci

Zákazníkem PostSignum QCA 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), které uzavírají s Českou poštou smlouvu o poskytování certifikačních služeb.

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

1.3.3.2 Pověřená osoba

Pověřenou 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 QCA a o jaký certifikát mají právo žádat (včetně typu certifikátu – politiky, podle které bude certifikát vydán).

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

1.3.3.3 Žadatel (podepisující nebo pečetící)

Žadatel o certifikát je zaměstnanec zákazníka – organizace nebo fyzická osoba, která má právo žádat o certifikát podle některé z platných certifikačních politik. Žadatel se přijmutím vydaného certifikátu stává podepisující osobou. Pečetící osobou se po přijmutí certifikátu stává zákazník.

1.3.4 Spoléhající se strany

Spoléhající se stranou je libovolná fyzická či právnická osoba spoléhající se na certifikát vydaný PostSignum QCA. 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:

Dodavatelé hardwaru, softwaru a datového připojení.

Ministerstvo práce a sociálních věcí ČR
IČ 00551023
Na Poříčním právu 1/376
128 01 Praha 2

Uvedený subjekt je dodavatelem identifikátoru klientů pro certifikační autoritu PostSignum QCA.

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 Qualified CA).

Komise pro certifikační politiky ČP zajišťuje:

- ustavuje Tým pro tvorbu certifikačních politik ČP, řídí a kontroluje jeho činnost,
- schvaluje nové certifikační politiky a v případě politik Root QCA rozhoduje o jejich zveřejnění,
- udržuje a kontroluje existující politiky,
- zodpovídá za konzistenci a integritu politik,
- schvaluje veškeré změny CPS,
- zodpovídá za publikování aktuální verze CPS,
- zodpovídá za konzistenci a integritu CPS.

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

Certifikáty vydávané PostSignum QCA mohou být použity

- k ověření elektronických podpisů (zaručených i kvalifikovaných) v souladu s [eIDAS],
- k ověření elektronických pečetí (zaručených i kvalifikovaných) v souladu s [eIDAS],
- k ověření elektronických značek v souladu se [ZSVD]
- k ověření certifikátů pro autentizaci internetových stránek v souladu s [eIDAS]

1.4.2 Omezení použití certifikátu

Omezení použití certifikátu je uvedené v příslušné certifikační politice. Obecně však platí, že certifikáty vydávané podle certifikačních politik PostSignum QCA nejsou primárně určené pro komunikace nebo transakce v oblastech se zvýšeným rizikem škod na zdraví nebo na majetku, jako jsou chemické provozy, letecký provoz, provoz jaderných zařízení apod. nebo v souvislosti s bezpečností a obranyschopností státu.

1.5 Správa politiky

Za iniciování změn v certifikační prováděcí směrnici nebo inicializaci vytvoření nové certifikační prováděcí směrnice je odpovědný Manažer CA. 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, které umožňuje danou verzi identifikovat.

Nová verze certifikační prováděcí směrnice bude zveřejněna formou interní směrnice České pošty. PAA ČP rozhodne, zda je nutné zveřejnit informaci o nové verzi certifikační prováděcí směrnice 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 příslušné certifikační politice.

1.5.1 Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

Za správu této certifikační provádějící směrnice je odpovědný poskytovatel certifikačních služeb, tedy Česká pošta, zastoupená pro tento účel Manažerem CA.

1.5.2 Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

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

manager.postsignum@cpost.cz

nebo na webových stránkách poskytovatele

www.postsignum.cz

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

Za správu této certifikační prováděcí směrnice a za její soulad s certifikačními politikami nebo za soulad s postupy jiných poskytovatelů certifikačních služeb odpovídá Manažer CA.

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), 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 QCA (např. změně postupů), která ovlivní obsah těchto dokumentů,
- pokud při pravidelné kontrole okolního prostředí PostSignum QCA 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 CA. Při přípravě změn v certifikační politice nebo v CPS rozhodne Manažer CA na základě seznamu identifikovaných změn, jakým způsobem budou plánované změny zveřejněny. Komise pro certifikační politiky podle potřeby ustanoví PCA ČP, kterému Manažer CA následně předá seznam požadovaných změn k zapracování.

Vypracované politiky nebo CPS předloží Manažer CA ke schválení Komisi pro certifikační politiky, která potom potvrdí OID (pouze politiky) a přidělí číslo verze.

1.6 Přehled použitých pojmů a zkratek

Certifikát Online – Aplikace, která slouží k vydání certifikátu prostřednictvím vzdálené identifikace.

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

Certifikát pro elektronickou pečeť – certifikát pro právnické osoby ve smyslu [eIDAS]

Coordinated Universal Time (UTC) – Koordinovaný světový čas, časový standard založený na Mezinárodním atomovém čase (TAI).

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

ECC – (Elliptic Curve Cryptography) je kryptografický algoritmus založený na eliptických křivkách. Konkrétní algoritmus je ECDSA.

DMZ – demilitarizovaná zóna

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 pro elektronický podpis – kvalifikovaný certifikát ve smyslu [eIDAS].

Kvalifikovaný certifikát pro elektronickou pečeť – kvalifikovaný certifikát ve smyslu [eIDAS].**Kvalifikovaný certifikát pro autentizaci internetových stránek -** kvalifikovaný certifikát ve smyslu [eIDAS]

Kvalifikované elektronické časové razítko – kvalifikované časové razítko ve smyslu [eIDAS].

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

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

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

NIA – Národní bod pro identifikaci a autentizaci je informační systém veřejné správy. Systém je určen pro bezpečné a zaručené vzdálené ověřování totožnosti uživatelů.

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

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

Orgán dohledu – Dohledový orgán nad kvalifikovanými poskytovateli služeb vytvářejících důvěru dle [eIDAS], který je stanoven na základě platných právních předpisů.

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

Ověřovací registrační autorita – zajišťuje vybrané služby registrační autority.

Párová data (klíčový pár) – Jsou základním primitivem asymetrické kryptografie. Tvoří je soukromý a veřejný klíč. Z hlediska důvěrnosti je potřebné chránit především jejich generování a soukromý klíč.

Pečetící osoba – osoba definovaná v [eIDAS]

PKI – Public Key Infrastructure – Infrastruktura veřejných klíčů

Platné právní předpisy – Jsou jimi myšleny právní předpisy upravující oblast elektronického podpisu, zejména potom Zákon o službách vytvářejících důvěru pro elektronické transakce 297/2016 Sb. a NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES včetně navazujících právních předpisů.

Podepisující osoba – osoba definovaná v [eIDAS].

PostSignum – hierarchie certifikačních autorit a autority časového razítka tvořená kořenovou certifikační autoritou PostSignum Root QCA, všemi podřízenými certifikačními autoritami, pro něž PostSignum Root QCA vydala certifikát, a autoritami časového razítka, pro které některá z certifikačních autorit PostSignum vydala kvalifikovaný certifikát pro elektronickou pečeť.

PostSignum QCA – hierarchie certifikačních autorit, vydávajících kvalifikované certifikáty ve smyslu [eIDAS].

PostSignum VCA – hierarchie certifikačních autorit, vydávajících komerční certifikáty.

PostSignum Root QCA – kořenová certifikační autorita, která má samo podepsaný kvalifikovaný certifikát pro elektronickou pečeť. Vydává certifikáty pro elektronickou pečeť pro podřízené certifikační autority a CRL. V hierarchii PostSignum mohou existovat další kořenové certifikační autority, které jsou navíc označeny pořadovým číslem, např. PostSignum Root QCA 2.

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

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

PostSignum TSA – autorita vydávající kvalifikovaná elektronická časová razítka ve smyslu [eIDAS]. Autoritu tvoří více jednotek (TSU). Každá jednotka má vlastní klíč a kvalifikovaný certifikát pro elektronickou pečeť.

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.

Prostředek pro elektronickou identifikaci – jedná se o prostředek, který slouží pro vzdálené prokázání totožnosti žadatele při využití aplikace Certifikát Online. Prostředek musí být s úrovní záruky „vysoká“ a musí být vydán v rámci kvalifikovaného systému elektronické identifikace v souladu s [ZoEI] a [eIDAS].

QCA ČP – viz PostSignum QCA.

QESCD – (Qualified Electronic Signature Creation Device) kvalifikovaný prostředek pro vytváření elektronických podpisů v souladu s [eIDAS]

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

Rozlišovací jméno – jednoznačně identifikuje podepisující, resp. pečetící osobu dle pravidel definovaných příslušnou certifikační politikou.

Soukromý klíč – souhrnné označení dat pro vytváření elektronického podpisu, dat pro vytváření elektronických pečetí, dat pro šifrování a dešifrování a dat pro autentizaci.

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

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

Uživatel certifikátu (relying party) – osoba, která užívá certifikát vydaný PostSignum například pro ověření elektronického podpisu či pečetě nebo pro zajištění jiných bezpečnostních služeb. Jinak též označována jako Osoba spoléhající se na certifikát.

VCA ČP – viz PostSignum VCA.

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

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

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

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

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

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

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

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

2. ODPOVĚDNOST ZA ZVEŘEJŇOVÁNÍ A ÚLOŽIŠTĚ INFORMACÍ A DOKUMENTACE

2.1 Úložiště informací a dokumentace

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

Za zveřejňování informací odpovídá Česká pošta jako poskytovatel certifikačních služeb.

2.2 Zveřejňování informací a dokumentace

Informace o vydaných certifikátech, o provozu PostSignum QCA a dokumentace PostSignum QCA jsou zveřejňovány v následujícím rozsahu:

2.2.1 Zveřejňování certifikátů a CRL

Certifikáty certifikačních autorit jsou zveřejňovány

- na webových stránkách poskytovatele,

  http://www.postsignum.cz

  http://www.postsignum.eu

- ve vydaných certifikátech je umístěn odkaz na vydávající certifikační autoritu ve formě rozšíření certifikátu (AuthorityInfoAccess).

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

- na webových stránkách poskytovatele

Certifikáty jsou publikovány ve formátech DER, PEM a TXT.

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

- na webových stránkách poskytovatele

Seznam zneplatněných certifikátů je publikován ve formátech DER, PEM a TXT. Povolený protokol je HTTP a HTTPS.

- na distribučních bodech seznamu zneplatněných certifikátů uvedených ve vydaném certifikátu (CRL Distribution Points)

2.2.2 Zveřejňování informací o certifikační autoritě

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

- webových stránkách poskytovatele, nebo

- obchodních místech (pouze k nahlédnutí).

Další důležité informace, zejména informace požadované platnými právními předpisy (např. odnětí akreditace, zneplatnění certifikátu pro elektronickou pečeť certifikační autority) nebo informace o mimořádné události jsou zveřejňovány

- na webových stránkách poskytovatele,
- na registračních autoritách ve formě vyvěšeného textového oznámení, nebo
- v celostátně distribuovaném deníku.

2.3 Periodicita zveřejňování informací

Informace o periodicitě zveřejňování jsou uvedeny v každé certifikační politice, obecně však platí, že:

- certifikační politiky, certifikační prováděcí směrnice a zpráva pro uživatele jsou zveřejňovány po schválení a vydání nové verze, vždy však před počátkem platnosti daného dokumentu (a v případě certifikační politiky před vydáním prvního certifikátu);
- certifikáty, pokud byly označeny pro zveřejnění, jsou zveřejňovány po jejich vydání do doby uvedené v certifikační politice;
- informace o zneplatněných certifikátech ve formě seznamu zneplatněných certifikátů (CRL) jsou zveřejňovány neprodleně po jejich vydání, nejpozději však před koncem platnosti posledního zveřejněného seznamu zneplatněných certifikátů. Nejpozději jednou za 24 hodin a zpravidla každé 4 hodiny nebo po každém zneplatnění certifikátu.
- důležité informace jsou zveřejňovány neprodleně.

2.4 Řízení přístupu k jednotlivým typům úložišť

Bližší informace o přístupu k informacím poskytovaným PostSignum QCA jsou uvedeny v každé certifikační politice, obecně však platí, že

- certifikační politiky, zpráva pro uživatele, certifikáty certifikačních autorit a informace o stavu certifikátu jsou přístupné pro čtení bez jakéhokoliv omezení;
- certifikáty koncových uživatelů, které byly určeny ke zveřejnění, jsou přístupné pro čtení bez jakéhokoliv omezení.

Poskytovatel certifikačních služeb neumožňuje neautorizovaný 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

Vzhledem k tomu, že PostSignum QCA 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 Požadavek na významovost jmen

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

3.1.3 Anonymita a používání pseudonymu

Obecně platí, ze PostSignum QCA nepodporuje vydávání anonymních certifikátů nebo certifikátů obsahujících pseudonym. Bližší informace jsou uvedeny v každé certifikační politice.

3.1.4 Pravidla pro interpretaci různých forem jmen

Vzhledem k tomu, že PostSignum QCA 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.

3.1.5 Jedinečnost jmen

Vzhledem k tomu, že PostSignum QCA 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 QCA 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.

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

3.1.6 Obchodní značky

Vzhledem k tomu, že PostSignum QCA vydává certifikáty pro různé subjekty podle různých certifikačních politik, nelze souhrnně a obecně definovat způsob, jakým je ošetřen případ vložení obchodních značek nebo registrovaných ochranných známek do certifikátu.

Obecně však platí, že všechna pole certifikátu, která PostSignum QCA ověřuje, mají předepsanou strukturu a musí být doložena jejich správnost a úplnost.

3.2 Počáteční ověření identity

3.2.1 Ověřování souladu dat, tj. postup při ověřování, zda má osoba data pro vytváření elektronických podpisů nebo pečetí (soukromý klíč) odpovídající datům pro ověřování elektronických podpisů nebo pečetí (veřejný klíč)

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 Ověřování identity právnické osoby nebo organizační složky státu

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

3.2.2.1 Uzavření smlouvy se zákazníkem – organizací

Zmocnění k podepisování za organizaci se prokazuje při uzavírání smlouvy o poskytování certifikačních služeb způsobem obvyklým v obchodním styku (konkrétní postupy jsou uvedené na webových stránkách poskytovatele).

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

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 Pre-registrace žadatelů o certifikát u zákazníka – organizace

Registrační autorita PostSignum QCA 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 QCA musí ověřit i tuto vazbu.

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

Pověřená osoba zasílá nebo předává poskytovateli certifikačních služeb seznam žadatelů, kteří mohou žádat o certifikát podle určité certifikační politiky. Seznam je podepsán pověřenou osobou, statutárním zástupcem nebo zmocněncem. Ověření podepsané osoby se provádí kontrolou totožnosti uvedené osoby v případě fyzického předání seznamu žadatelů nebo kontrolou elektronického podpisu této osoby pomocí osobního certifikátu vydaného PostSignum v případě elektronického předání seznamu žadatelů.

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.

3.2.2.3 Změna pověřené osoby

V době platnosti smlouvy se zákazníkem – organizací může dojít ke změně ve jmenování pověřených osob. Změna musí být zachycena v dodatku smlouvy, kde bude uvedena nová pověřená osoba a její podpisový vzor.

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.

Typy dokladů, které lze předložit při ověření identity jsou uvedeny v konkrétní certifikační politice.

Pracovník registrační autority zkontroluje:

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

Podnikající fyzická osoba nebo zaměstnanec organizace může prokázat svou totožnost i na dálku s využitím Prostředku pro elektronickou identifikaci. K tomuto způsobu prokázání totožnosti slouží aplikace Certifikát Online, která je umístěná na webových stránkách poskytovatele.

Podnikající fyzická osoba nebo zaměstnanec organizace mohou prokázat svou totožnost i jiným způsobem popsaným v příslušné certifikační politice.

3.2.3.2 Ověřování identity nepodnikající fyzické osoby

Fyzická osoba, jakožto nepodnikající jednotlivec, 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.

Nepodnikající fyzická osoba může prokázat svou totožnosti i na dálku s využitím Prostředku pro elektronickou identifikaci. K tomuto způsobu prokázání totožnosti slouží aplikace Certifikát Online, která je umístěná na webových stránkách poskytovatele.

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.

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.

Smlouva může být uzavřena taktéž elektronickou formou v aplikaci Certifikát Online.

Česká pošta uzavírá se zákazníkem smlouvu o poskytování certifikačních služeb za podmínek definovaných obchodním zákoníkem. (konkrétní postupy jsou uvedené na webových stránkách poskytovatele)

3.2.4 Neověřené informace vztahující se k držiteli certifikátu nebo podepisující či pečetící osobě

Podrobný seznam informací o zákazníkovi nebo žadateli včetně informace, zdali je daná informace ověřovaná a jakým způsobem, je uveden v certifikační politice. Obecně platí, že Česká pošta jako poskytovatel certifikačních služeb požaduje doložení většiny identifikačních údajů uvedených ve smlouvě nebo v certifikátu.

3.2.5 Ověřování specifických práv

Viz příslušná certifikační politika.

3.2.6 Kritéria pro interoperabilitu

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

Spolupráce s jinými certifikačními autoritami provozovanými stejným poskytovatelem certifikačních služeb je možná zejména na úrovni vydání certifikátu podřízené certifikační autority autoritou PostSignum Root QCA a za podmínek definovaných v příslušné certifikační politice.

3.3 Identifikace a autentizace při zpracování požadavků na výměnu dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických pečetí v certifikátu

3.3.1 Identifikace a autentizace při rutinní výměně dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí a jim odpovídajících dat ověřování elektronických podpisů nebo dat pro ověřování elektronických pečetí (dále „párová data“)

Při rutinní výměně párových dat (vydání následného certifikátu) není vyžadována fyzická přítomnost žadatele na pracovišti registrační autority. O vydání následného certifikátu se žádá elektronickou cestou. Žadatel se autentizuje použitím elektronického podpisu založeného na certifikátu vydaném PostSignum definovaným v příslušné certifikační politice.

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 kapitola 3.2.3).

Při zpracování žádosti o následný certifikát, při níž se žadatel autentizoval použitím elektronického podpisu založeného na zneplatněném certifikátu, v tom případě bude žádost zamítnuta registrační autoritou.

3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu

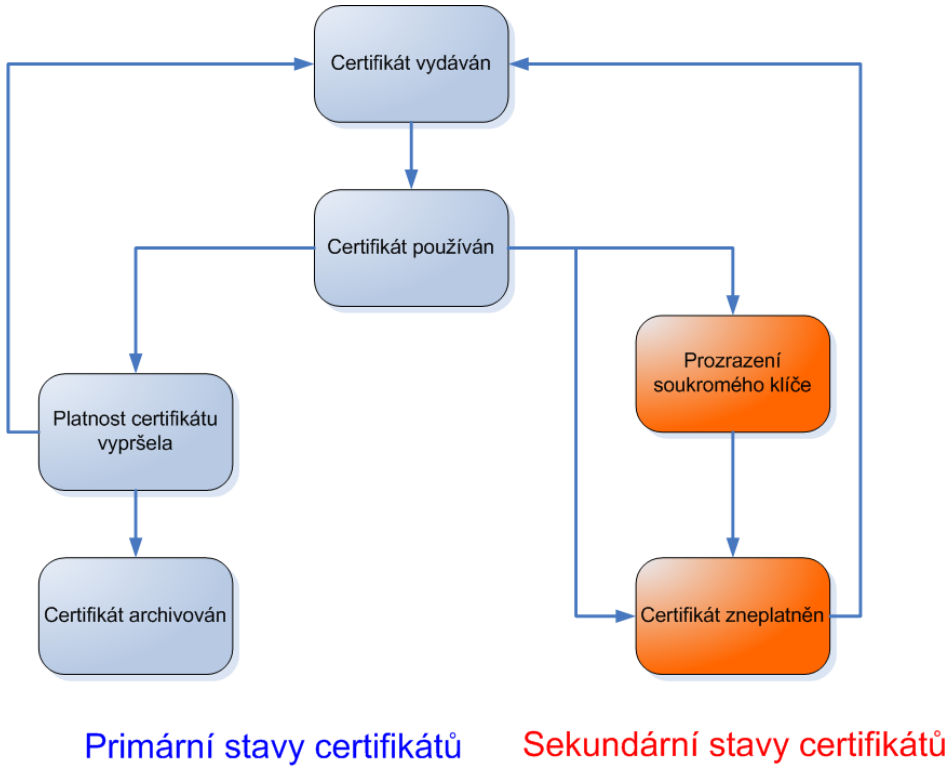
Žadatel nebo držitel certifikátu se při žádosti o zneplatnění certifikátu autentizuje

- znalostí hesla pro zneplatnění, které zadal (nebo mu bylo vygenerováno) při registraci žádosti o certifikát,
- osobním dokladem obdobně jako při registraci žádosti o certifikát, nebo
- elektronickým podpisem, založeným na certifikátu vydaném podřízenou certifikační autoritou z hierarchie PostSignum, na elektronicky zaslané žádosti o zneplatnění certifikátu, nebo
- na dálku s využitím Prostředku pro elektronickou identifikaci.

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

4. POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

Životní cyklus certifikátů vydávaných PostSignum QCA je znázorněn na následujícím obrázku:



Obrázek reprezentuje na nejvyšší úrovni správu certifikátů v rámci PostSignum QCA. 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 QCA procházejí těmito primárními stavy.

Sekundární stavy certifikátu jsou tyto:

- prozrazení soukromého klíče,
- certifikát zneplatněn.

Sekundární stavy představují výjimečné situace, proto se předpokládá, že

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

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

4.1 Žádost o vydání certifikátu

Postupy registrace žádosti o certifikát jsou definovány v příslušné certifikační politice.

4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu

PostSignum QCA 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 (zaměstnanec organizace nebo osoba definovaná organizací) k registrační autoritě s elektronickou žádostí o certifikát a s příslušnými doklady.

- Zákazníky – fyzické osoby, které si chtějí nechat vydat certifikáty pro sebe jakožto podepisující nebo pečetící osobu. 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 Registrační proces a odpovědnosti poskytovatele a žadatele

Vlastní proces registrace, požadavky na tento proces a odpovědnosti poskytovatele a žadatele jsou popsány v příslušné certifikační politice.

4.2 Zpracování žádosti o certifikát

Postupy zpracování žádosti o certifikát jsou definovány v příslušné certifikační politice.

4.2.1 Identifikace a autentizace

Před zpracováním žádosti musí být žadatel o certifikát identifikován a musí být provedena jeho autentizace. Konkrétní požadavky na proces identifikace a autentizace jsou definovány v příslušné certifikační politice.

4.2.2 Přijetí nebo zamítnutí žádosti o certifikát

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

4.2.3 Doba zpracování žádosti o certifikát

Doba zpracování žádosti o certifikát je definována v příslušné certifikační politice. Obecně však platí, že certifikát je vydán zpravidla v den podání žádosti.

4.3 Vydání certifikátu

Postupy vydání certifikátu jsou definovány v příslušné certifikační politice.

4.3.1 Úkony CA v průběhu vydávání certifikátu

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

4.3.2 Oznámení o vydání certifikátu držiteli certifikátu, podepisující nebo pečetící

Seznam subjektů informovaných o vydání certifikátu je uveden v příslušné certifikační politice. Obecně však platí, že o vydání certifikátu informuje poskytovatel certifikačních služeb žadatele o certifikát.

4.4 Převzetí vydaného certifikátu

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

4.4.1 Úkony spojené s převzetím certifikátu

Certifikát je zpravidla vydán žadateli krátce po schválení žádosti a jejím vložení do systému certifikační autority. Žadatel přebírá vydaný certifikát pomocí URL zaslanému žadateli o certifikát. Žadatel přistoupí na webovou stránku nacházející se na zaslaném 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.

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

4.4.2 Zveřejňování vydaných certifikátů poskytovatelem

Certifikát, u kterého byl držitelem vysloven souhlas se zveřejněním, je do 24 hodin od převzetí zveřejněn na webových stránkách poskytovatele.

4.4.3 Oznámení o vydání certifikátu jiným subjektům

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

Toto ustanovení se netýká předávání seznamu všech vydaných kvalifikovaných certifikátů na základě žádosti orgánu dohledu.

4.5 Použití párových dat a certifikátu

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

4.5.1 Použití dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí a certifikátu držitelem certifikátu, podepisující nebo pečetící osobou

Žadatel o certifikát (podepisující nebo pečetící) vydaný PostSignum QCA je oprávněn používat soukromý klíč a odpovídající certifikát pouze pro účely specifikované v certifikační politice, podle které byl daný certifikát vydán.

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

Spoléhající se strana je oprávněna použít certifikát vydaný PostSignum QCA pouze pro účely a za podmínek specifikovaných v příslušné certifikační politice, podle které byl daný certifikát vydán.

4.6 Obnovení certifikátu

PostSignum QCA tuto službu neposkytuje.

4.6.1 Podmínky pro obnovení certifikátu

PostSignum QCA tuto službu neposkytuje.

4.6.2 Subjekty oprávněné požadovat obnovení certifikátu

PostSignum QCA tuto službu neposkytuje.

4.6.3 Zpracování požadavku na obnovení certifikátu

PostSignum QCA tuto službu neposkytuje.

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

PostSignum QCA tuto službu neposkytuje.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu

PostSignum QCA tuto službu neposkytuje.

4.6.6 Zveřejňování vydaných obnovených certifikátů poskytovatelem

PostSignum QCA tuto službu neposkytuje.

4.6.7 Oznámení o vydání obnoveného certifikátu jiným subjektům

PostSignum QCA tuto službu neposkytuje.

4.7 Výměna dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických pečetí v certifikátu

Služba výměny dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických pečetí v certifikátu je označována jako vydání následného certifikátu. Toto označení bude dále používáno i dále v textu.

Vydání následného certifikátu probíhá způsobem definovaným certifikační politikou. Obecně platí, že žádost o vydání následného certifikátu je podepsána zaručeným elektronickým podpisem a je odeslána na centrální registrační autoritu. Vydaný certifikát je poté dostupný na webových stránkách poskytovatele, kde je prováděna jeho akceptace a stažení.

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

Podmínky pro vydání následného certifikátu jsou uvedeny v příslušné certifikační politice.

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

Seznam subjektů, které mohou žádat o vydání následného certifikátu je uveden v příslušné certifikační politice.

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

Postupy registrace žádosti o obnovu certifikátu jsou definovány v příslušné certifikační politice.

4.7.4 Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických pečetí podepisující nebo pečetící

Seznam subjektů informovaných o vydání certifikátu je uveden v příslušné certifikační politice. Obecně však platí, že o vydání certifikátu informuje poskytovatel certifikačních služeb žadatele o certifikát.

4.7.5 Úkony spojené s převzetím certifikátu s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických pečetí

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

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

Pro zveřejňování následných certifikátů platí stejná pravidla jako pro zveřejňování prvotního certifikátu vydaného obvyklým způsobem (viz kapitola 4.4.2).

4.7.7 Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických pečetí jiným subjektům

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

4.8 Změna údajů v certifikátu

Podmínky pro změnu údajů v certifikátu jsou definovány v příslušné certifikační politice. Obecně platí, že dojde ke zneplatnění stávajícího certifikátu a k vydání prvotního certifikátu s novými údaji obvyklým způsobem (viz kapitola 4.3).

4.8.1 Podmínky pro změnu údajů v certifikátu

Podmínky pro změnu údajů v certifikátu jsou definovány v příslušné certifikační politice. Obecně platí, že dojde-li ke změně údajů v certifikátu vydaného PostSignum QCA, musí držitel certifikátu tuto změnu neprodleně ohlásit poskytovateli certifikačních služeb.

4.8.2 Subjekty oprávněné požadovat změnu údajů v certifikátu

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

certifikátech zaměstnanců pověřená osoba, a to buď elektronicky, 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, elektronicky nebo písemně.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

Zpracování požadavku na změnu údajů v certifikátu je definováno v příslušné certifikační politice.

4.8.4 Oznámení o vydání certifikátu se změněnými údaji podepisující nebo pečetící

Vydání certifikátu se změněnými údaji je shodné s vydáním prvotního certifikátu obvyklým způsobem a pro oznamování jsou použita odpovídající ustanovení (viz kapitola 4.3.2).

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Vydání certifikátu se změněnými údaji je shodné s vydáním prvotního certifikátu obvyklým způsobem a pro přebírání jsou použita odpovídající ustanovení (viz kapitola 4.4.1).

4.8.6 Zveřejňování vydaných certifikátů se změněnými údaji

Vydání certifikátu se změněnými údaji je shodné s vydáním prvotního certifikátu obvyklým způsobem a pro zveřejňování jsou použita odpovídající ustanovení (viz kapitola 4.4.2).

4.8.7 Oznámení o vydání certifikátu se změněnými údaji jiným subjektům

Vydání certifikátu se změněnými údaji je shodné s vydáním prvotního certifikátu obvyklým způsobem a pro oznamování jiným subjektům jsou použita odpovídající ustanovení (viz kapitola 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

Obecně se jedná o případy, kdy existuje riziko zneužití vydaného a platného certifikátu. Nejčastější důvody pro zneplatnění certifikátu jsou uvedeny v příslušné certifikační politice.

4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

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

Zneplatnění certifikátu může iniciovat Manažer CA jakožto zástupce certifikační autority, která vydala certifikát, nebo zástupce orgánu dohledu.

4.9.3 Požadavek na zneplatnění certifikátu

Postup a způsob vznesení požadavku na zneplatnění certifikátu jsou popsány v příslušné certifikační politice.

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 obsluhou PostSignum QCA do zveřejnění CRL obsahujícího příslušný certifikát nepřesáhne 24 hodin.

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

Povinnosti spoléhajících se stran jsou uvedeny v příslušné certifikační politice. Obecně však platí, že spoléhající se strany musí před použitím certifikátu ověřit jeho stav vůči aktuálnímu CRL zveřejněnému na webových stránkách poskytovatele.

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů (CRL) kořenové certifikační autority PostSignum Root QCA je vydáván minimálně jednou ročně.

Seznam zneplatněných certifikátů (CRL) podřízených certifikačních autorit v hierarchii PostSignum je vydáván po každém zneplatnění certifikátu nebo jednou za 24 hodin, zpravidla každé 4 hodiny.

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

Všechny postupy, procesy a havarijní plány jsou nastaveny tak, aby služba vydávání seznamu zneplatněných certifikátů zůstala zachována a doba uvedená v kapitolách 4.9.4, 4.9.5 a 4.9.7 byla dodržena.

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

PostSignum QCA tuto službu poskytuje jako veřejně dostupnou bezplatnou službu, která je poskytována dle standardu RFC 6960. Profil certifikátu je uveden v politice pro vydávání certifikátů OCSP a profil žádosti a odpovědi OCSP jsou uvedeny v kapitole 7 tohoto dokumentu.

4.9.10 Požadavky při ověřování statutu certifikátu on-line

Viz ustanovení v kapitole 4.9.9.

4.9.11 Jiné způsoby oznamování zneplatnění certifikátu

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

4.9.12 Případné odlišnosti postupu zneplatnění v případě kompromitace dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí

Postup pro zneplatnění certifikátu v případě kompromitace dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí je shodný s obecným postupem pro zneplatnění certifikátu.

4.9.13 Podmínky pro pozastavení platnosti certifikátu

PostSignum QCA tuto službu neposkytuje.

4.9.14 Subjekty oprávněné požadovat pozastavení platnosti certifikátu

PostSignum QCA tuto službu neposkytuje.

4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu

PostSignum QCA tuto službu neposkytuje.

4.9.16 Omezení doby pozastavení platnosti certifikátu

PostSignum QCA tuto službu neposkytuje.

4.10 Služby související s ověřováním statutu certifikátu

Stav certifikátu je možné ověřit

- na seznamu zneplatněných certifikátů (CRL) v rámci služby zveřejňující veřejné informace PostSignum QCA protokolem HTTP,
- v rámci služby vyhledávání vydaných certifikátů přístupné na webových stránkách poskytovatele (neplatí pro certifikáty vydávané PostSignum Root QCA), nebo
- pomocí služby OCSP.

4.10.1 Funkční charakteristiky

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

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

Primárním zdrojem aktuálního CRL jsou webové stránky poskytovatele.

V rámci služby vyhledávání vydaných certifikátů přístupné na webových stránkách poskytovatele 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 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.

Dostupnost služby OCSP je 7 dní v týdnu 24 hodin denně.

4.10.3 Další charakteristiky služeb statutu certifikátu

Další charakteristiky služeb statutu certifikátu nejsou stanoveny.

4.11 Ukončení poskytování služeb pro držitele certifikátu, podepisující nebo pečetící osobu,

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

4.12 Úschova dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí u důvěryhodné třetí strany a jejich obnova

Soukromé klíče držitelů certifikátů jsou generovány a uschovávány žadatelem o certifikát. Jedná se o klíče pro algoritmus RSA a ECDSA, povolená délka klíče je definována v příslušné certifikační politice. PostSignum QCA s těmito klíči nepřichází do styku, není zodpovědná za jejich ochranu ani zálohování.

4.12.1 Politika a postupy při úschově a obnovování dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí

PostSignum QCA tuto službu neposkytuje.

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

PostSignum QCA tuto službu neposkytuje.

5. MANAGEMENT, PROVOZNÍ A FYZICKÁ BEZPEČNOST

Pro PostSignum QCA byly zpracovány dokumenty:

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

Zmíněné dokumenty byly vypracovány na základě výsledků provedené analýzy rizik.

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

5.1 Fyzická bezpečnost

Podrobný popis požadavků a opatření z oblasti fyzické bezpečnosti je uveden v dokumentu Systémová bezpečnostní politika [SBP].

5.1.1 Umístění a konstrukce

V PostSignum QCA 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 (typicky obchodní místa certifikační autority) a
- pracoviště ověřovací registrační autority (typicky kontaktní místa veřejné správy).

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.

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 ověřovací registrační autority a mobilní registrační autority se vztahují režimová opatření definovaná v Systémové bezpečnostní politice [SBP].

5.1.3 Elektřina a klimatizace

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

5.1.4 Vlivy vody

Centrální pracoviště jsou umístěna mimo zátopové oblasti.

Prostory centrálních pracovišť jsou vybaveny signalizací zatopení vodou. 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 QCA jsou k dispozici trezory.

5.1.7 Nakládání s odpady

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

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

5.1.8 Zálohy mimo budovu

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

5.2 Procesní bezpečnost

Podrobný popis požadavků a opatření z oblasti procesní bezpečnosti a přidělování rolí je uveden v dokumentu Organizační zajištění úlohy QCA [OZU], v dokumentu Systémová bezpečnostní politika [SBP] a interní dokumentaci PostSignum QCA.

5.2.1 Důvěryhodné role

Viz příslušná certifikační politika.

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

Viz příslušná certifikační politika.

5.2.3 Identifikace a autentizace pro každou roli

Viz příslušná certifikační politika.

5.2.4 Role vyžadující rozdělení povinností

Viz příslušná certifikační politika.

5.3 Personální bezpečnost

Podrobný popis požadavků a opatření z oblasti personální bezpečnosti a přidělování rolí je uveden v dokumentu Organizační zajištění úlohy QCA [OZU] a v dokumentu Systémová bezpečnostní politika [SBP].

5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

Viz příslušná certifikační politika.

5.3.2 Posouzení spolehlivosti osob

Viz příslušná certifikační politika.

5.3.3 Požadavky na přípravu pro výkon role, vstupní školení

Viz příslušná certifikační politika.

5.3.4 Požadavky a periodicita školení

Viz příslušná certifikační politika.

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

Viz příslušná certifikační politika.

5.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

Viz příslušná certifikační politika.

5.3.8 Dokumentace poskytovaná zaměstnancům

Viz příslušná certifikační politika.

5.4 Auditní záznamy (logy)

Viz příslušná certifikační politika.

5.4.1 Typy zaznamenávaných událostí

Viz příslušná certifikační politika.

5.4.2 Periodicita zpracování záznamů

Viz příslušná certifikační politika.

5.4.3 Doba uchování auditních záznamů

Viz příslušná certifikační politika.

5.4.4 Ochrana auditních záznamů

Viz příslušná certifikační politika.

5.4.5 Postupy pro zálohování auditních záznamů

Viz příslušná certifikační politika.

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

Viz příslušná certifikační politika.

5.4.7 Postup při oznamování události subjektu, který ji způsobil

Viz příslušná certifikační politika.

5.4.8 Hodnocení zranitelnosti

Viz příslušná certifikační politika.

5.5 Uchovávání informací a dokumentace

Viz příslušná certifikační politika.

5.5.1 Typy informací a dokumentace, které se uchovávají

Viz příslušná certifikační politika.

5.5.2 Doba uchování uchovávaných informací a dokumentace

Viz příslušná certifikační politika.

5.5.3 Ochrana úložiště uchovávaných informací a dokumentace

Viz příslušná certifikační politika.

5.5.4 Postupy při zálohování uchovávaných informací a dokumentace

Viz příslušná certifikační politika.

5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

Viz příslušná certifikační politika.

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

Viz příslušná certifikační politika.

5.5.7 Postupy pro získání a ověření uchovávaných informací a dokumentace

Viz příslušná certifikační politika.

5.6 Výměna dat pro ověřování elektronických pečetí v nadřízeném kvalifikovaném certifikátu poskytovatele

Viz příslušná certifikační politika.

5.7 Obnova po havárii nebo kompromitaci

Viz příslušná certifikační politika.

5.7.1 Postup v případě incidentu a kompromitace

Viz příslušná certifikační politika.

5.7.2 Poškození výpočetních prostředků, softwaru nebo dat

Viz příslušná certifikační politika.

5.7.3 Postup při kompromitaci dat pro vytváření elektronických pečetí poskytovatele

5.7.3.1 Kompromitace soukromého klíče podřízené certifikační autority

Viz příslušná certifikační politika.

5.7.3.2 Kompromitace soukromého klíče PostSignum Root QCA

Viz příslušná certifikační politika.

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 QCA 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 QCA věcí rozhodnutí managementu České pošty. O rozhodnutí managementu musí být s minimální prodlevou informováni všichni zákazníci PostSignum QCA.

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

5.8 Ukončení činnosti CA nebo RA

5.8.1 Ukončení činnosti kořenové certifikační autority

Viz příslušná certifikační politika.

5.8.2 Ukončení činnosti podřízené certifikační autority

Viz příslušná certifikační politika.

5.8.3 Ukončení činnosti registrační autority

Viz příslušná certifikační politika.

5.8.4 Ukončení činnosti poskytovatele certifikačních služeb

Viz příslušná certifikační politika.

5.8.5 Odnětí akreditace

Viz příslušná certifikační politika.

6. TECHNICKÁ BEZPEČNOST

Podrobný popis požadavků a opatření z oblasti technické bezpečnosti je uveden v dokumentu Systémová bezpečnostní politika [SBP]; nastavení systémů PostSignum QCA a opatření ve formě postupů jsou popsány v interní dokumentaci PostSignum QCA.

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Postup generování párových dat je popsán v příslušné certifikační politice.

6.1.2 Předání dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí podepisující nebo pečetící osobě

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

6.1.3 Předání dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických pečetí poskytovateli certifikačních služeb

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

6.1.4 Poskytování dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických pečetí certifikační autoritou spoléhajícím se stranám

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

6.1.5 Délky párových dat

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

Klíče certifikačních autorit v hierarchii PostSignum mají pro algoritmus RSA délku modulu minimálně 4096 bitů a pro algoritmus ECDSA délku pLen a qLen 512 bitů, konkrétně křivka P-521 (secp521r1). Klíče držitelů certifikátů mají pro algoritmus RSA a ECDSA délku modulu definovanou v příslušné certifikační politice.

6.1.6 Generování parametrů dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických pečetí a kontrola jejich kvality

Postup generování parametrů dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických pečetí a kontrola jejich kvality je popsán v příslušné certifikační politice.

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

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

6.2 Ochrana dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí a bezpečnost kryptografických modulů

6.2.1 Standardy a podmínky používání kryptografických modulů

Standardy a podmínky používání kryptografických modulů jsou popsány v příslušné certifikační politice.

6.2.2 Sdílení tajemství

Sdílení tajemství je popsáno v příslušné certifikační politice.

6.2.3 Úschova dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí

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

6.2.4 Zálohování dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí

K šifrování soukromého klíče je použit symetrický algoritmus AES. Zašifrované klíče jsou uložené na pevném disku zařízení obsahujícího příslušný kryptografický modul. Zálohovat tyto klíče může jedna osoba; obnovit do aktivovaného modulu, ze kterého zálohy pocházejí, také.

6.2.5 Uchovávání dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí

Uchovávání dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí je popsáno v příslušné certifikační politice.

6.2.6 Transfer dat pro vytváření elektronických pečetí do kryptografického modulu nebo z kryptografického modulu

Transfer dat pro vytváření elektronických pečetí do kryptografického modulu nebo z kryptografického modulu je popsán v příslušné certifikační politice.

6.2.7 Uložení dat pro vytváření elektronických pečetí v kryptografickém modulu

Uložení dat pro vytváření elektronických pečetí v kryptografickém modulu je popsán v příslušné certifikační politice.

6.2.8 Postup při aktivaci dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí

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 dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí

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 dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí

Postup při zničení dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí je popsán v příslušné certifikační politice.

6.2.11 Hodnocení kryptografických modulů

Hodnocení kryptografických modulů je popsáno v příslušné certifikační politice.

6.3 Další aspekty správy párových dat

6.3.1 Uchovávání dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických pečetí

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

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

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

6.4 Aktivační data

V systému PostSignum QCA jsou používána aktivační data různého charakteru, například přístupová hesla, PIN a jiné. Všechny aspekty týkající se aktivačních dat, jejich generování, instalace a používání, jsou popsány v 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 prozrazením neoprávněné osobě. Příslušné povinnosti v tomto smyslu mají všichni pracovníci PostSignum QCA 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

Specifické technické požadavky na počítačovou bezpečnost jsou popsány v příslušné certifikační politice.

6.5.2 Hodnocení počítačové bezpečnosti

Hodnocení počítačové bezpečnosti je popsáno v příslušné certifikační politice.

6.6 Bezpečnost životního cyklu

6.6.1 Řízení vývoje systému

Řízení vývoje systému je popsán v příslušné certifikační politice.

6.6.2 Kontroly řízení bezpečnosti

Kontroly řízení bezpečnosti jsou popsány v příslušné certifikační politice.

6.6.3 Řízení bezpečnosti životního cyklu

Řízení bezpečnosti životního cyklu je popsáno v příslušné certifikační politice.

6.7 Síťová bezpečnost

Síťová bezpečnost je popsána v příslušné certifikační politice.

6.8 Časová razítka

Viz kapitola 5.5.5.

7. PROFILY CERTIFIKÁTU, SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ A OCSP

7.1 Profil certifikátu

PostSignum QCA vydává certifikáty 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 QCA podporuje rozšiřující položky popsané v odpovídajících certifikačních politikách. Certifikační autorita si vyhrazuje právo vložit do certifikátu další položky, pokud si to vyžádá změna právních předpisů nebo norem, které upravují činnost poskytovatelů certifikačních služeb.

7.1.1 Číslo verze

PostSignum QCA vydává certifikáty vyhovující standardu X.509 verze 3.

7.1.2 Rozšiřující položky v certifikátu

V certifikátech se používají rozšíření specifikovaná v jednotlivých certifikačních politikách.

7.1.3 Objektové identifikátory (dále „OID“) algoritmů

Algoritmům používaným v PostSignum QCA nejsou přiřazeny OID. V hierarchii PostSignum QCA se nepoužívají specifické algoritmy, které by vyvíjel provozovatel PostSignum QCA nebo jeho dodavatel, ale pouze algoritmy odpovídající požadavkům platných standardů.

7.1.4 Způsoby zápisu jmen a názvů

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

V certifikátech vydávaných PostSignum QCA jsou podporovány následující znakové sady:

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

7.1.5 Omezení jmen a názvů

Použitá jména musí být přesnou transkripcí údajů poskytovatele certifikačních služeb nebo zákazníka žádajícího o vydání certifikátu, tj. musí být totožná s požadovanou resp. doložitelnou předlohou.

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

7.1.6 OID 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 QCA nepoužívá.

7.1.8 Syntaxe a sémantika rozšiřující položky kvalifikátorů politiky „Policy Qualifiers“

Rozšiřující položka „Policy Qualifier“ obsahuje odkaz na webové stránky poskytovatele, kde lze získat certifikační politiku, podle které byl certifikát vydán, a textovou informaci o skutečnosti, že certifikát byl vydán jako kvalifikovaný certifikát pro elektronický podpis nebo kvalifikovaný certifikát pro elektronickou pečeť nebo kvalifikovaný certifikát pro autentizaci internetových stránek dle [eIDAS].

7.1.9 Způsob zápisu kritické rozšiřující položky „Certificate Policies“

Způsob zápisu rozšiřující položky „Certificate Policies“ je uveden v příslušné certifikační politice. Tato položka není označena jako kritická.

7.2 Profil seznamu zneplatněných certifikátů

7.2.1 Číslo verze

V PostSignum QCA jsou vydávány seznamy zneplatněných certifikátů podle standardu X.509 verze 2.

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

Podrobný profil CRL je uveden v certifikační politice. Obecně platí, že v seznamech zneplatněných certifikátů se používají následující rozšiřující položky:

- Authority Key Identifier (KeyIdentifier, AuthorityCertIssuer + AuthorityCertSerialNumber),
- CRL Number,
- Revocation Reason (u jednotlivého záznamu o certifikátu),
- Invalidity Date (u jednotlivého záznamu o certifikátu; volitelně).

7.3 Profil OCSP

Profil certifikátu OCSP je uveden v certifikační politice pro vydání certifikátu OCSP, která je zveřejněna na webových stránkách poskytovatele.

Struktura OCSP žádosti – OCSP Request Data

Název položky	**Popis**	**Hodnota/příznak použití**
Version	Verze protokolu OCSP (povinná položka)	1
Requestor List		
Certificate ID	údaje o dotazovaném certifikátu – položka se může opakovat	
Hash Algorithm	hash žádosti	SHA-1
Issuer Name Hash	hash vypočítaný ze jména vydavatele certifikátu	
Issuer Key Hash	hash vypočítaný z otisku veřejného klíče vydavatele certifikátu	
Serial Number	sériové číslo dotazovaného certifikátu	
Request Extensions		

OCSP Nonce	Náhodné, jednou vygenerované číslo (64 bitů). Je-li obsaženo v žádosti, pak ho obsahuje i odpověď. (nepovinná položka)	

Žádost OCSP nemusí být podepsaná.

Struktura OCSP odpovědi – OCSP Response Data

Název položky	**Popis**	**Hodnota/příznak použití**
OCSP Response Status	Přirozené číslo, označující stav odpovědi	0 – successful 1 – malformedRequest 2 – internalError 3 – tryLater 6 – unauthorized
Response Type	Basic OCSP Response	
Version	Verze protokolu OCSP	1
Responder Id	DN podpisového certifikátu OCSP responderu	
Produced At	Čas podpisu odpovědi OCSP responderu v UTC	
Responses:		
Certificate ID	Údaje odpovídají údajům v žádosti	
Cert Status	Stav certifikátu. good – certifikát je platný revoked – certifikát je zneplatněný unknown – stav certifikátu je neznámý (např. takový certifikát neexistuje)	0 – good 1 – revoked 2 – unknown
Revocation Time	Čas revokace certifikátu. Položka je uvedena pouze v případě Cert Status=revoked	
Revocation Reason	Důvod revokace certifikátu. Položka je uvedena pouze v případě Cert Status=revoked	
This Update	Čas v UTC, od něhož je indikován stav odpovědi.	
Response Extensions		
OCSP Nonce	Náhodné, jednou vygenerované číslo (64 bitů). Je-li obsaženo v žádosti, pak ho obsahuje i odpověď. (nepovinná položka)	

7.3.1 Číslo verze
Viz kapitola 7.3

7.3.2 Rozšiřující položky OCSP
Viz kapitola 7.3

8. HODNOCENÍ SHODY A JINÁ HODNOCENÍ

Oblast hodnocení shody je podrobněji rozvedena v dokumentu Auditní a archivační politika, který je přílohou Systémové bezpečnostní politiky [SBP].

8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

8.1.1 Interní kontrola

Nejméně jednou za dvanáct měsíců je pracovníky odboru interní audit a řízení rizik

- 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.

Součástí této kontroly je provedení částečné kontroly bezpečnostní shody ve smyslu platných právních předpisů.

O provedení každé interní kontroly musí být vypracována podepsaná písemná zpráva. Přílohou této zprávy je zpráva o částečné kontrole bezpečnostní shody ve smyslu platných právních předpisů. Zpráva je archivována stejným způsobem jako ostatní záznamy o provozu PostSignum QCA a uchovávána nejméně po dobu deseti let.

8.1.2 Externí kontrola

Bezpečnost a integrita systémů a procesů PostSignum QCA je ověřena externí kontrolou provedenou auditorem nezávislým na České poště v rozsahu celkové kontroly stanovenou platnými právními předpisy.

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

8.2 Identita a kvalifikace hodnotitele

Viz příslušná certifikační politika.

8.3 Vztah hodnotitele k hodnocenému subjektu

Viz příslušná certifikační politika.

8.4 Hodnocené oblasti

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 skutečnost, zda

- poskytovatel provozuje důvěryhodné systémy v souladu s platnými právními předpisy a příslušnými standardy,

- poskytovatel provádí změny v důvěryhodných systémech v souladu s bezpečnostní dokumentací poskytovatele, a to s jejími částmi upravujícími řízení změn.

8.5 Postup v případě zjištění nedostatků

Viz příslušná certifikační politika.

8.6 Sdělování výsledků hodnocení

Viz příslušná certifikační politika.

9. OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

Platný ceník je zveřejněn na webových stránkách poskytovatele.

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

Platný ceník je zveřejněn na webových stránkách poskytovatele.

9.1.5 Jiná ustanovení týkající se poplatků (vč. refundací)

Žádná ustanovení v této kapitole.

9.2 Finanční odpovědnost

9.2.1 Krytí pojištěním

Viz příslušná certifikační politika.

9.2.2 Další aktiva a záruky

Viz příslušná certifikační politika.

9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

PostSignum QCA tuto službu neposkytuje.

9.3 Citlivost obchodních informací

9.3.1 Výčet citlivých informací

Za citlivé informace jsou v obchodním styku považovány veškeré důvěrné informace, okolnosti a údaje, které se jedna zúčastněných stran dozvěděla v souvislosti s plněním smlouvy o poskytování certifikačních služeb a o kterých nebylo písemně dohodnuto mezi smluvními stranami, že mohou být zveřejněny.

Za citlivé informace jsou vždy považovány informace označené jako

- interní
- obchodní tajemství
- důvěrná informace
- ostatní chráněné informace

9.3.2 Informace mimo rámec citlivých informací

Viz příslušná certifikační politika.

9.3.3 Odpovědnost za ochranu citlivých informací

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

9.4 Ochrana osobních údajů

Česká pošta zajišťuje ochranu osobních údajů osob, k nimž získá přístup při poskytování certifikačních služeb. Zásady ochrany osobních údajů jsou obsaženy v certifikačních politikách, všeobecných obchodních podmínkách ČP [VOP] a vycházejí z příslušných ustanovení zákona č. 110/2019 Sb., o zpracování osobních údajů, v platném znění.

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

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 Práva 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 poskytovatele. ČP je nositelem následujících registrací doménových jmen, souvisejících s poskytováním certifikační autority: postsignum.cz.

9.6 Zastupování a záruky

Česká pošta jako poskytovatel certifikačních služeb zaručuje, že splní veškeré povinnosti uložené smlouvou se zákazníkem, certifikační politikou, interními předpisy a mandatorními 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

9.6.1.1 Záruky PostSignum Root QCA

Certifikační autorita PostSignum Root QCA zaručuje, že

- bude věnovat náležitou péči všem činnostem spojeným s poskytováním certifikačních služeb; náležitá péče zahrnuje provoz v souladu
  - s interní provozní dokumentací,
  - příslušnou certifikační politikou,
  - touto certifikační prováděcí směrnicí,
  - systémovou bezpečnostní politikou,
  - platnými právními předpisy,
- bude udržovat tuto certifikační prováděcí směrnici,
- bude ve sféře své působnosti vynucovat dodržování pravidel popsaných v této certifikační prováděcí směrnici,
- zveřejní certifikační politiku, podle které vydává certifikáty a která je určená ke zveřejnění, na webových stránkách poskytovatele, případně jinými vhodnými způsoby,
- zveřejní samo podepsaný certifikát i otisk samo podepsaného certifikátu alespoň dvěma na sobě nezávislými způsoby,
- bez zbytečných odkladů posoudí žádost o certifikát, vydá rozhodnutí, zda bude certifikát vydán, a o tomto rozhodnutí bude informovat žadatele,
- vydá certifikát vyhovující standardu X.509 a splňující požadavky žadatele,
- vydá 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,
- bude informovat žadatele o tom, že certifikát byl vydán, a předá vydaný certifikát žadateli,
- zveřejní certifikát, který byl akceptován žadatelem, bez zbytečných odkladů na webových stránkách poskytovatele, případně jiným vhodným způsobem,
- zneplatní certifikáty podle pravidel popsaných v certifikační politice,
- informuje držitele certifikátu o tom, že jeho certifikát byl zneplatněn z vůle certifikační autority nebo z vůle orgánu dohledu,
- zveřejní seznam zneplatněných certifikátů bez zbytečného prodlení, ve lhůtě uvedené v certifikační politice,
- prověří podezření, že došlo k prozrazení soukromého klíče v rámci působnosti PostSignum Root QCA, což by mohlo vést ke ztrátě důvěryhodnosti této certifikační autority,
- bude asistovat při kontrole, kterou provádí externí auditor nebo pověřený pracovník České pošty,

- zajistí bezpečný provoz systémů podle požadavků platných právních předpisů.

9.6.1.2 Záruky podřízených certifikačních autorit

Podřízená certifikační autorita působící v hierarchii PostSignum QCA zaručuje, že

- bude věnovat náležitou péči všem činnostem spojeným s poskytováním certifikačních služeb; náležitá péče zahrnuje provoz v souladu
  - s interní provozní dokumentací,
  - příslušnou certifikační politikou,
  - touto certifikační prováděcí směrnicí,
  - systémovou bezpečnostní politikou,
  - platnými právními předpisy,
- posoudí a schválí zřízení registrační autority, která spadá do její působnosti,
- ve sféře své působnosti bude vynucovat dodržování pravidel popsaných v této certifikační prováděcí směrnici,
- zveřejní certifikační politiky, podle kterých vydává certifikáty, na svých webových stránkách, případně jinými vhodnými způsoby,
- bez zbytečných odkladů posoudí žádost o certifikát, vydá rozhodnutí, zda bude certifikát vydán, a o tomto rozhodnutí informuje žadatele,
- vydá certifikát vyhovující standardu X.509 a splňující požadavky zákazníka,
- vydá 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,
- informuje žadatele o tom, že certifikát byl vydán, a předá vydaný certifikát žadateli,
- zveřejní certifikát, u kterého byl vysloven souhlas se zveřejněním a který byl akceptován žadatelem, bez zbytečných odkladů na svých webových stránkách, případně jiným vhodným způsobem,
- zneplatní certifikát podle pravidel popsaných v certifikační politice,
- informuje držitele certifikátu o tom, že jeho certifikát byl zneplatněn z vůle certifikační autority,
- informuje držitele certifikátu o tom, že jeho certifikát byl zneplatněn z vůle orgánu dohledu,
- zveřejní seznam zneplatněných certifikátů bez zbytečného prodlení, ve lhůtě uvedené v certifikační politice,
- prověří podezření, že došlo k prozrazení soukromého klíče v rámci působnosti podřízené certifikační autority, což by mohlo vést ke ztrátě důvěryhodnosti této certifikační autority,

- bude asistovat při kontrole, kterou provádí externí auditor nebo pověřený pracovník České pošty,
- zajistí bezpečný provoz systémů podle požadavků platných právních předpisů.

9.6.2 Zastupování a záruky RA

Registrační autorita působící v hierarchii PostSignum QCA zaručuje, že

- bude věnovat náležitou péči všem činnostem spojeným s poskytováním certifikačních služeb; náležitá péče zahrnuje provoz v souladu
  - se smlouvou mezi Českou poštou a danou registrační autoritou, pokud jsou provozovatelé certifikační autority a registrační autority různé právní subjekty,
  - s interní provozní dokumentací,
  - příslušnou certifikační politikou,
  - touto certifikační prováděcí směrnicí,
  - systémovou bezpečnostní politikou,
  - platnými právními předpisy,
- ve sféře své působnosti bude vynucovat dodržování pravidel popsaných v této certifikační prováděcí směrnici,
- bude přijímat žádosti o certifikát včetně odpovídajících písemných dokladů, schvalovat žádosti nebo je zamítat podle pravidel daných příslušnou certifikační politikou,
- poučí žadatele o jeho povinnostech vyplývajících z příslušné certifikační politiky, poskytne žadateli tuto certifikační politiku nebo informaci, kde lze certifikační politiku získat,
- postoupí 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,
- postoupí ke zpracování žádost o certifikát odpovídající standardu X.509 a splňující náležitosti vyžadované příslušnou certifikační politikou,
- ověří totožnost žadatele o certifikát v souladu s příslušnou certifikační politikou,
- bez zbytečných odkladů posoudí žádost o certifikát, vydá rozhodnutí, zda bude certifikát vydán, a o tomto rozhodnutí informuje žadatele,
- informuje žadatele o tom, že certifikát byl vydán a předá, resp. zajistí předání vydaného certifikátu žadateli,
- zajistí zneplatnění certifikátu podle pravidel popsaných v certifikační politice,
- vede evidenci žádostí o certifikát, které byly jejich prostřednictvím podány,

- prověří podezření, že došlo k prozrazení soukromého klíče v rámci působnosti dané registrační autority, což může vést ke ztrátě důvěryhodnosti dané registrační autority,

- zajistí pořizování evidence dokladů spojených s přijetím a zpracováním žádosti a vydáním certifikátu,

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

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

9.6.3 Zastupování a záruky držitele certifikátu, podepisující nebo pečetící osoby

Viz příslušná certifikační politika.

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 kvalifikovaného certifikátu. Tyto povinnosti jsou uvedeny v příslušných certifikačních politikách. Obecně platí, že spoléhající se strana musí zejména

- Získat certifikáty PostSignum Root QCA a podřízené certifikační autority z bezpečného zdroje (webové stránky poskytovatele, případně webové stránky orgánu dohledu) a ověřit otisk („fingerprint“) těchto certifikátů.

- Před použitím certifikátu vydaného podřízenou certifikační autoritou v hierarchii PostSignum 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 podřízenou certifikační autoritou podle této politiky vhodný pro účel, ke kterému jej chce použít.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Viz příslušná certifikační politika.

9.7 Zřeknutí se záruk

Viz příslušná certifikační politika.

9.8 Omezení odpovědnosti

Ujednání o omezení odpovědnosti je uvedeno v příslušné certifikační politice, [VOP] nebo v objednávce služeb (resp. smlouvě o poskytování služeb).

9.9 Odpovědnost za škodu, náhrada škody

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

9.10 Doba platnosti, ukončení platnosti

9.10.1 Doba platnosti

Počátek platnosti tohoto dokumentu je určen dnem vydání uvedeným v kapitole 1.2

Konec platnosti tohoto dokumentu je určen dnem ukončení platnosti.

9.10.2 Ukončení platnosti

Viz příslušná certifikační politika.

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

Viz příslušná certifikační politika.

9.11.2 Komunikace v rámci systému PostSignum QCA

Viz příslušná certifikační politika.

9.11.3 Komunikační jazyk

Viz příslušná certifikační politika.

9.12 Změny

9.12.1 Postup při změnách

Postupy pro zapracování změn jsou uvedeny v kapitole 1.5.

9.12.2 Postup při oznamování změn

Vydání nové certifikační prováděcí směrnice bude oznámeno v aktualitách na webových stránkách poskytovatele.

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 QCA.

OID jsou přiřazeny:

- PostSignum Root QCA,
- každé certifikační autoritě, které PostSignum Root QCA vydala certifikát, zejména certifikační autoritě PostSignum Qualified CA,

- každé certifikační politice, podle které jsou vydávány certifikáty v rámci PostSignum QCA.

OID nejsou přiřazeny registračním autoritám ani 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 QCA,
  - 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 a vydaném certifikátu,
- v interních dokumentech České pošty.

Jakákoliv změna v certifikační politice vyvolá změnu verze dokumentu; větší změna v certifikační politice, která má dopad na použitelnost certifikátu, záruky, odpovědnost nebo procesy, vyvolá i změnu OID.

9.13 Řešení sporů

Viz příslušná certifikační politika.

9.14 Rozhodné právo

Činnost PostSignum QCA se řídí právním řádem České republiky.

9.15 Shoda s právními předpisy

Činnost PostSignum QCA je v souladu s platnými právními předpisy České republiky.

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

Struktura této certifikační prováděcí směrnice je v souladu se strukturou uvedenou v RFC 3647.

9.16 Další ustanovení

9.16.1 Rámcová dohoda

Žádná ustanovení v této kapitole.

9.16.2 Postoupení práv

Viz příslušná certifikační politika.

9.16.3 Oddělitelnost ustanovení

Viz příslušná certifikační politika.

9.16.4 Zřeknutí se práv

Příslušná ustanovení se neuplatní.

9.16.5 Vyšší moc

Viz příslušná certifikační politika.

9.16.6 Přístupnost pro osoby se zdravotním postižením

Viz příslušná certifikační politika.

9.17 Další opatření

9.17.1 Řídící dokumenty

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

[eIDAS]	NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ESETSI EN 119 312Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
[ETSI EN 319 401]	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ETSI EN 319 411]	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1 – 3
[ETSI EN 319 412]	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1 – 5
[ETSI EN 119 312]	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
[ISO 27001]	ČSN ISO/IEC 27001:2014 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky
[RFC 6960]	Internet X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
[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
[Z110]	Zákon č. 110/2019 Sb. o zpracování osobních údajů v aktuálním znění
[ZoEP]	Zákon č. 227/2000 Sb. o elektronickém podpisu (zrušen zákonem 297/2016 Sb.)
[ZoSVD]	Zákon č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce v platném znění

[ZoEI] Zákon č. 250/2017 Sb. o elektronické identifikaci v platném znění

9.17.2 Odkazy a literatura

[VOP] Všeobecné obchodní podmínky certifikačních služeb

V tomto dokumentu je odkazováno rovněž na následující interní dokumenty:

[OZU] Předpis ČP „Organizační zajištění úloh certifikačních autorit a autority časových razítek České pošty, s.p.“ – příloha č. 2 „Organizační zajištění úlohy Kvalifikovaná certifikační autorita České pošty, s.p.“ v aktuálním znění

[SBP] Předpis ČP „Systémová bezpečnostní politika certifikačních autorit a autority časových razítek České pošty, s.p.“ – příloha č. 2 „ Systémová bezpečnostní politika pro úlohu Kvalifikovaná certifikační autorita České pošta, s.p.“ v aktuálním znění