

Certifikační politika PostSignum Qualified CA pro kvalifikované certifikáty pro elektronický podpis

Verze 2.1.0

OBSAH

1 Úvod	5
1.1 Přehled	5
1.2 Název a jednoznačné určení dokumentu	5
1.3 Participující subjekty	6
1.4 Použití certifikátu	7
1.5 Správa politiky	7
1.6 Přehled použitých pojmů a zkratk	8
2 Odpovědnost za zveřejňování a úložiště informací a dokumentace	12
2.1 Úložiště informací a dokumentace	12
2.2 Zveřejňování informací a dokumentace	12
2.3 Periodicita zveřejňování informací	13
2.4 Řízení přístupu k jednotlivým typům úložišť	13
3 Identifikace a autentizace	14
3.1 Pojmenování	14
3.2 Počáteční ověření identity	15
3.3 Identifikace a autentizace při zpracování požadavků na výměnu dat pro ověřování elektronických podpisů	17
3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu	17
4 Požadavky na životní cyklus certifikátu	19
4.1 Žádost o vydání certifikátu	19
4.2 Zpracování žádosti o certifikát	22
4.3 Vydání certifikátu	23
4.4 Převzetí vydaného certifikátu	23
4.5 Použití párových dat a certifikátu	24
4.6 Obnovení certifikátu	25
4.7 Výměna dat pro ověřování elektronických podpisů v certifikátu	25
4.8 Změna údajů v certifikátu	26
4.9 Zneplatnění a pozastavení platnosti certifikátu	27
4.10 Služby související s ověřováním statutu certifikátu	31
4.11 Ukončení poskytování služeb pro držitele certifikátu nebo podepisující osobu	32
4.12 Úschova dat pro vytváření elektronických podpisů u důvěryhodné třetí strany a jejich obnova	32
5 Management, provozní a fyzická bezpečnost	33
5.1 Fyzická bezpečnost	33
5.2 Procesní bezpečnost	34
5.3 Personální bezpečnost	35
5.4 Auditní záznamy (logy)	36
5.5 Uchovávání informací a dokumentace	37
5.6 Výměna dat pro ověřování elektronických pečeti v nadřazeném certifikátu pro elektronickou pečeť poskytovatele	38
5.7 Obnova po havárii nebo kompromitaci	39
5.8 Ukončení činnosti CA nebo RA	40
6 Technická bezpečnost	42

6.1 Generování a instalace párových dat	42
6.2 Ochrana dat pro vytváření elektronických podpisů, dat pro vytváření elektronických značek nebo dat pro ověřování elektronických pečeti a bezpečnost kryptografických modulů.....	43
6.3 Další aspekty správy párových dat.....	45
6.4 Aktivační data	45
6.5 Počítačová bezpečnost	45
6.6 Bezpečnost životního cyklu	46
6.7 Síťová bezpečnost	46
6.8 Časová razítka	46
7 Profily certifikátu, seznamu zneplatněných certifikátů a OCSP	47
7.1 Profil certifikátu	47
7.2 Profil seznamu zneplatněných certifikátů	51
7.3 Profil OCSP.....	51
8 Hodnocení shody a jiná hodnocení	53
8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení	53
8.2 Identita a kvalifikace hodnotitele	53
8.3 Vztah hodnotitele k hodnocenému subjektu	53
8.4 Hodnocené oblasti.....	53
8.5 Postup v případě zjištění nedostatků	53
8.6 Sdělování výsledků hodnocení.....	53
9 Ostatní obchodní a právní záležitosti	54
9.1 Poplatky	54
9.2 Finanční odpovědnost	54
9.3 Citlivost obchodních informací.....	54
9.4 Ochrana osobních údajů.....	55
9.5 Práva duševního vlastnictví	56
9.6 Zastupování a záruky	56
9.7 Zřeknutí se záruk.....	56
9.8 Omezení odpovědnosti.....	57
9.9 Odpovědnost za škodu, náhrada škody	57
9.10 Doba platnosti, ukončení platnosti.....	57
9.11 Komunikace mezi zúčastněnými subjekty	57
9.12 Změny	58
9.13 Řešení sporů.....	59
9.14 Rozhodné právo	59
9.15 Shoda s právními předpisy	59
9.16 Další ustanovení.....	59
9.17 Další opatření	60

Evidence revizí a změn

Verze	Datum revize	Důvod a popis změny	Autor	Schválil
1.0	1. 7. 2016	První verze	PCA ČP	PAA ČP
1.1	2. 10. 2017	Změny v souvislosti s akreditací dle eIDAS	PCA ČP	PAA ČP
2.0	20. 6. 2019	Změny v souvislosti s novou kořenovou CA	PCA ČP	PAA ČP
2.0	1. 9. 2020	Revize dokumentu - žádná změna	PCA ČP	
2.1.0	1. 9. 2021	Změny: - přidání nového způsobu ověření prostřednictvím vzdálené identifikace	PCA ČP	PAA ČP

1 ÚVOD

Tento dokument stanoví pravidla a postupy pro vydávání kvalifikovaných certifikátů pro elektronický podpis (dále také jen certifikát). Jméno osoby, užívající vydaný certifikát, je uvedeno ve jménu certifikátu. Certifikáty jsou vydávány zákazníkům, resp. zaměstnancům zákazníků (organizací), které stanoví zástupce organizace.

1.1 Přehled

Česká pošta, s.p. (dále i Česká pošta či ČP) provozuje certifikační autoritu s názvem PostSignum QCA.

Při vydávání certifikátů koncovým uživatelům uplatňuje model tzv. pre-registrace zákazníka, jehož cílem je minimalizovat účast statutárního zástupce organizace v celém procesu a vyžadovat minimální množství dokladů od osob, jež si budou žádat o certifikát.

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

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

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

Kvalifikované certifikáty vydané podle této certifikační politiky jsou určeny pro osoby, které jsou samotným zákazníkem nebo v určitém vztahu k zákazníkovi, který uzavírá s Českou poštou smlouvu o poskytování certifikačních služeb. Osoby, které žádají o certifikáty vydané podle této politiky a užívají je, budou v souladu s platnými právními předpisy nazývány podepisujícími osobami. Držitelem certifikátu je zákazník České pošty.

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

Certifikáty vydané podle této certifikační politiky mohou být použity pouze pro ověření elektronického podpisu podepisující osoby v souladu s platnými právními předpisy.

Odpovídající soukromý klíč k vydanému certifikátu dle této certifikační politiky může být uložen na QESCD, ale není to vyžadováno.

Plnění zásad této politiky rozpracovává a zajišťuje aktuální Certifikační prováděcí směrnice PostSignum QCA.

1.2 Název a jednoznačné určení dokumentu

Tab. 1 Identifikace politiky

Název dokumentu	Certifikační politika PostSignum Qualified CA pro kvalifikované certifikáty pro elektronický podpis
Verze dokumentu	2.1.0
Stav	finální

OID poskytovatele certifikačních služeb	2.23.134
OID PostSignum Root QCA	2.23.134.1.4.2.1
OID PostSignum Qualified CA	2.23.134.1.4.2.2
OID této politiky	2.23.134.1.4.1.17.210
Datum vydání	15. 11. 2021
Datum účinnosti	15. 12. 2021
Doba platnosti	Do odvolání nebo do dne ukončení služeb autorit PostSignum QCA.

1.3 Participující subjekty

Podřízené certifikační autority mohou být řízeny a provozovány pouze Českou poštou (s výjimkou registračních autorit - viz dále).

Identifikační a kontaktní údaje poskytovatele certifikačních služeb jsou:

Česká pošta, s.p.

IČ 47114983, DIČ CZ47114983

Politických vězňů 909/4, 225 99 Praha 1

tel.: 954 301 111

e-mail: info@cpost.cz

Česká pošta je akreditovaným poskytovatelem certifikačních služeb na základě akreditace udělené Ministerstvem informatiky ČR dne 3.8.2005.

Česká pošta se dne 1. 7. 2016 stala kvalifikovaným poskytovatelem služeb vytvářejících důvěru v souladu s [eIDAS].

1.3.1 Certifikační autority (dále „CA“)

Úkolem CA PostSignum QCA je především vydávat a spravovat certifikáty certifikačních autorit PostSignum Root QCA, PostSignum Qualified CA a zákazníků České pošty v souladu s definovanými certifikačními politikami.

1.3.2 Registrační autority (dále „RA“)

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

Registrační autority zajišťují zejména tyto služby:

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

- spravují a provozují kvalifikované prostředky pro vytváření elektronických podpisů (pouze vybrané externí subjekty).

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

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

Pro účely vydání certifikátu prostřednictvím vzdálené identifikace slouží centrální registrační autorita.

1.3.3 Držitelé kvalifikovaných certifikátů a podepisující osoby, kteří požádali o vydání kvalifikovaného certifikátu (dále certifikátu), a kterým byl certifikát vydán.

1.3.4 Spoléhající se strany

Spoléhající se stranou je libovolný subjekt spoléhající se na certifikát vydaný PostSignum QCA. Spoléhající se strany nevstupují do smluvního vztahu s poskytovatelem certifikačních služeb.

1.3.5 Jiné participující subjekty

Certifikační autorita PostSignum QCA může využívat pro zajištění poskytování služeb externí subjekty.

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

Kvalifikované certifikáty vydané podle této certifikační politiky mohou být použity pouze pro ověření elektronického podpisu podepisující osoby v souladu s platnými právními předpisy.

1.4.2 Omezení použití certifikátu

Kvalifikované certifikáty vydávané podle této certifikační politiky nejsou primárně určené pro komunikace nebo transakce v oblastech se zvýšeným rizikem škod na zdraví nebo na majetku, jako jsou chemické provozy, letecký provoz, provoz jaderných zařízení apod. nebo v souvislosti s bezpečností a obranyschopností státu. Česká pošta je připravena diskutovat se zákazníkem zvláštní podmínky poskytování certifikačních služeb ve výše uvedených sektorech.

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

1.5 Správa politiky

1.5.1 Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

Za správu této certifikační politiky je odpovědný poskytovatel certifikačních služeb, tedy Česká pošta, konkrétně Manažer CA.

1.5.2 Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

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

manager.postsignum@cpost.cz

nebo na webových stránkách poskytovatele.

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

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

1.5.4 Postupy při schvalování souladu podle 1.5.3

Tento dokument je vytvářen týmem pro tvorbu certifikačních politik ČP, který je dle potřeby ustavován Komisí pro certifikační politiky ČP, je jí řízen a kontrolován.

Vypracovanou politiku předloží Manažer CA ke schválení Komisi pro certifikační politiky, která potvrdí OID politiky a přidělí číslo verze.

1.6 Přehled použitých pojmů a zkratek

Akreditace – Pod pojmem akreditace je myšleno získání statutu kvalifikovaného poskytovatele služeb vytvářejících důvěru dle [eIDAS].

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.

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 certifikační politiky a certifikační prováděcí směrnice, 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].

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

Manažer CA – osoba v řídicí 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 vyžadována 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.

Podpisující 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 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 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 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 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 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 pečeteť 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 – <http://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.

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.

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

Vydané certifikáty jsou uloženy v databázi certifikační autority.

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

2.2.1 Zveřejňování certifikátů a CRL

Certifikáty certifikačních autorit jsou zveřejňovány

- na webových stránkách poskytovatele

www.postsignum.cz,

www.postsignum.eu, nebo

- na obchodních místech České pošty, kde je možné požádat o jejich zkopírování na přinesené médium.

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

- na webových stránkách poskytovatele.

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

- na webových stránkách poskytovatele, nebo

- na distribučních bodech seznamu zneplatněných certifikátů uvedených ve vydaném certifikátu (CDP).

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 obchodních místech a registračních autoritách ve formě vyvěšeného textového oznámení,

- v celostátně distribuovaném deníku.

2.3 Periodicita zveřejňování informací

Informace jsou zveřejňovány v následujících intervalech:

- certifikační politiky, certifikační prováděcí směrnice a zpráva pro uživatele jsou zveřejňovány po schválení a vydání nové verze.
- certifikáty, pokud byly označeny pro zveřejnění, jsou zveřejňovány elektronickou cestou nejpozději do 24 hodin od přijetí certifikátu;
- 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.
- důležité informace, zejména informace požadované platnými právními předpisy jsou zveřejňovány neprodleně.

2.4 Řízení přístupu k jednotlivým typům úložišť

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

Poskytovatel certifikačních služeb neumožňuje neautorizovaný přístup k vydaným certifikátům, u kterých nebyl držitelem vysloven souhlas se zveřejněním.

3 IDENTIFIKACE A AUTENTIZACE

3.1 Pojmenování

3.1.1 Typy jmen

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

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

3.1.1.1 Identifikátor klienta MPSV

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

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

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

3.1.2 Požadavek na významovost jmen

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

3.1.3 Anonymita a používání pseudonymu

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

3.1.4 Pravidla pro interpretaci různých forem jmen

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

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

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

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

3.1.5 Jedinečnost jmen

Každá osoba v systému certifikační autority má přiřazen jedinečný identifikátor, který je uložen v údaji „serialNumber“ v Subjectu certifikátu. Zákazníci (s výjimkou nepodnikajících fyzických osob) dále přiřazují každému žadateli o certifikát číslo.

V položce Subject certifikátu je uvedena kombinace jednoznačných údajů o zákazníkovi (IČO zákazníka a jméno zákazníka) a jednoznačných údajů o žadateli o certifikát, čímž je zaručeno, že dvěma různými žadateli nebudou vydány certifikáty se stejnou položkou Subject.

V případě kolize rozlišovacích jmen dvou žadatelů o certifikát, a tím i kolize položky Subject v certifikátech těchto dvou osob, rozhodne o řešení Manažer CA a toto řešení navrhne pověřeným osobám zákazníků (resp. zákazníkům) neprodleně od vzniku kolize.

3.1.6 Obchodní značky

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

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

3.2 Počáteční ověření identity

3.2.1 Ověřování souladu dat, tj. postup při ověřování, zda má osoba data pro vytváření elektronických podpisů odpovídající datům pro ověřování elektronických podpisů

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

3.2.2 Ověřování identity právnické osoby nebo organizační složky státu

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

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

3.2.3 Ověřování identity fyzické osoby

3.2.3.1 Ověřování identity podnikající fyzické osoby nebo zaměstnance organizace

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

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

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

Identita může být ověřena také na dálku s využitím Prostředku pro elektronickou identifikaci.

3.2.3.2 Ověřování identity nepodnikající fyzické osoby

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

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

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

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

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

Identita může být ověřena také na dálku s využitím Prostředku pro elektronickou identifikaci.

3.2.4 Neověřené informace vztahující se k držiteli certifikátu nebo podepisující osobě

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

Česká pošta, jakožto poskytovatel certifikačních služeb, dále neověřuje správnost údajů

- funkce žadatele v rámci zákazníka,
- organizační jednotka, kde žadatel o certifikát pracuje,
- číslo zaměstnance,

uvedených v seznamu žadatelů, který předává poskytovateli certifikačních služeb pověřená osoba zákazníka.

3.2.5 Ověřování specifických práv

Žádná ustanovení v této kapitole.

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.

3.3 Identifikace a autentizace při zpracování požadavků na výměnu dat pro ověřování elektronických podpisů

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

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

- certifikační politiky PostSignum Qualified CA pro kvalifikované osobní certifikáty verze 1.0 a vyšší nebo
- certifikační politiky PostSignum Qualified CA pro kvalifikované certifikáty pro elektronický podpis verze 1.0 a vyšší.

3.3.2 Identifikace a autentizace při výměně párových dat po zneplatnění certifikátu

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

3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu

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

- znalostí hesla pro zneplatnění, které zadal 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
- jedním osobním dokladem v případě zaměstnance organizace či podnikající fyzické osoby, nebo jedním osobním dokladem a jedním doplňujícím dokladem v případě nepodnikající fyzické osoby (viz kapitola 3.2.3), nebo
- na dálku s využitím Prostředku pro elektronickou identifikaci.

Pověřená osoba prokáže svou totožnost:

- podpisem písemné žádosti o zneplatnění certifikátu, nebo
- elektronickým podpisem, založeným na certifikátu vydaném podřízenou certifikační autoritou z hierarchie PostSignum, na elektronicky zaslané žádosti o zneplatnění certifikátu, nebo

- osobním dokladem při podání žádosti o zneplatnění certifikátu osobně na registrační autoritě České pošty; pracovník registrační autority dále ověřuje, zda se pověřená osoba nachází na aktuálním seznamu pověřených osob, nebo
- autentizací do aplikace Zákaznický portál na webových stránkách poskytovatele.

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

O zneplatnění kvalifikovaného certifikátu může požádat orgán dohledu. Oprávněným žadatelem o zneplatnění kvalifikovaného certifikátu je v tomto případě zástupce orgánu dohledu.

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

4.1 Žádost o vydání certifikátu

4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu

Žádost o vydání certifikátu podle této certifikační politiky mohou podat:

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

4.1.2 Registrační proces a odpovědnosti poskytovatele a žadatele

4.1.2.1 Uzavření smlouvy

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

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

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

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

Smlouva o poskytování certifikačních služeb obsahuje mimo jiné:

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

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

Fyzické osoby (podnikající a nepodnikající) mohou uzavřít taktéž smlouvu na dálku prostřednictvím aplikace Certifikát Online. Podrobné informace o tomto způsobu jsou uvedeny na webové stránce poskytovatele.

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

4.1.2.2 Pre-registrace žadatelů o certifikát

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

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

Dále pověřená osoba nebo samotný zákazník určují, zdali může být vydaný certifikát zveřejněn široké veřejnosti bez omezení.

Registrační autorita ověřuje totožnost žadatele o certifikát pomocí dokladů uvedených v kapitole 3.2 nebo na dálku s využitím Prostředku pro elektronickou identifikaci. Vazbu mezi žadatelem a zákazníkem (organizací) uvedeným v certifikátu garantuje pověřená osoba zákazníka (organizace), která spravuje seznam žadatelů předávaný poskytovateli certifikačních služeb.

4.1.2.3 Odpovědnost zákazníka

Zákazník je povinen zejména:

- poskytovat pravdivé a úplné informace při uzavírání smlouvy o poskytování certifikačních služeb,
- neprodleně uvědomit poskytovatele certifikačních služeb o změnách údajů, které jsou ve smlouvě uvedeny, zejména o změnách údajů o pověřených osobách,
- neprodleně informovat poskytovatele certifikačních služeb o změnách údajů zákazníka, které jsou uvedeny v certifikátu. Podle charakteru změny poskytovatel certifikačních služeb rozhodne, zda je třeba zneplatnit platné certifikáty, které byly pro zákazníka vydány,
- umožnit poskytovateli certifikačních služeb přístup k QESCD, pokud je QESCD pod správou poskytovatele certifikačních služeb a je na něm uložený soukromý klíč a odpovídající certifikát vydaný dle této certifikační politiky.

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

4.1.2.4 Odpovědnost pověřených osob

Pověřená osoba je povinna zejména:

- poskytovat pravdivé a úplné informace o žadatelích oprávněných žádat o certifikát podle této politiky,
- neprodleně uvědomit poskytovatele certifikačních služeb o změnách údajů, které udržuje v seznamech žadatelů o certifikát.

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

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

4.1.2.5 Odpovědnost žadatele

Žadatel (podepisující osoba) je povinen zejména:

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

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

4.1.2.6 Odpovědnost poskytovatele

Poskytovatel certifikačních služeb je zejména povinen:

- v procesu registrace zákazníka a žadatele o certifikát ověřit všechny údaje podle předložených dokladů,
- v nejkratším možném termínu od podání žádosti posoudit žádost o certifikát resp. žádost o následný certifikát, vydat rozhodnutí, zda bude certifikát vydán, v případě zamítnutí žádosti o tomto rozhodnutí informovat žadatele nebo zákazníka,
- vydat certifikát obsahující věcně správné údaje na základě informací, které jsou certifikační autoritě k dispozici v době vydávání certifikátu,
- v případě žádosti o certifikát, jehož soukromý klíč byl vygenerován na QESCD, se prokazatelně o této skutečnosti přesvědčit a vložit do certifikátu příslušný příznak, že soukromý klíč je uložen na QESCD,
- spravovat a provozovat QESCD, u kterého je stanoveno, že je možné ho spravovat a provozovat pouze kvalifikovaným poskytovatelem služeb vytvářejících důvěru a zároveň obsahuje soukromý klíč a odpovídající certifikát vydaný dle této certifikační politiky (správa a provoz QESCD probíhá na základě dohodnutých podmínek mezi zákazníkem a poskytovatelem),
- zveřejňovat certifikační politiky, podle kterých vydává certifikáty, na webových stránkách poskytovatele, případně jinými vhodnými způsoby (viz kapitola 2.2),
- zveřejnit certifikát pro elektronickou pečeť poskytovatele certifikačních služeb tak, aby se každý mohl ujistit o jeho identitě,
- věnovat náležitou péči všem činnostem spojeným s poskytováním certifikačních služeb; náležitá péče zahrnuje provoz v souladu
 - s platnými právními předpisy,
 - s touto certifikační politikou,
 - s certifikační prováděcí směrnicí,
 - se systémovou bezpečnostní politikou,
 - s provozní dokumentací.

4.2 Zpracování žádosti o certifikát

4.2.1 Identifikace a autentizace

4.2.1.1 Fyzická identifikace

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

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

Žadatel o certifikát má možnost sdělit heslo pro případné zneplatnění certifikátu, pokud to systém registrační autority umožňuje. V případě žádosti o následný certifikát může být heslo pro zneplatnění zasláno v šifrované formě. Heslo musí splňovat požadavky (min. 8 znaků, z toho min. jedno malé písmeno, min. jedno velké písmeno, min. jednu číslici a min. jeden neabecední znak). Pokud žadatel heslo nesdělí nebo nebude splňovat uvedené požadavky, bude vygenerováno automaticky systémem. Heslo pro zneplatnění certifikátu je vždy uvedeno v protokolu o vydání certifikátu.

Pracovník registrační autority zkontroluje totožnost žadatele o certifikát na základě předloženého osobního dokladu a v případě, že to platné právní předpisy vyžadují, vytvoří a uloží kopie osobního dokladu žadatele o certifikát. Oproti seznamu žadatelů ověří, zda daná osoba skutečně smí žádat o certifikát dle dané certifikační politiky.

4.2.1.2 Identifikace na dálku

Žadatel o certifikát se autentizuje pomocí Prostředku pro elektronickou identifikaci do webové aplikace Certifikát Online a dále postupuje dle pokynů aplikace.

Při využití aplikace Certifikát Online si nemůže žadatel zvolit vlastní heslo pro zneplatnění, ale toto heslo mu je vygenerováno automaticky. Heslo pro zneplatnění je vždy uvedeno na Protokolu o vydaném certifikátu.

4.2.2 Přijetí nebo zamítnutí žádosti o certifikát

4.2.2.1 Přijetí nebo zamítnutí žádosti o první certifikát

Žadatel poskytne registrační autoritě elektronickou žádost ve formátu PKCS#10 obsahující veřejný klíč formou ID žádosti, která byla předtím uložena do systému poskytovatele. Elektronickou žádost na výměnném médiu může registrační autorita odmítnout.

Do certifikátu budou vloženy údaje dle platného seznamu žadatelů.

Pokud jsou všechny údaje odsouhlaseny žadatelem, registrační autorita schválí vydání certifikátu, v opačném případě bude žádost registrační autoritou zamítnuta.

Pokud má registrační autorita pochybnosti o identifikaci žadatele nebo pokud se vyskytnou jiné nesrovnalosti, odmítne vydat certifikát a o této skutečnosti informuje žadatele o certifikát.

Podrobné informace ohledně způsobu podání žádosti o první certifikát jsou uvedeny na webových stránkách poskytovatele.

4.2.2.2 Přijetí nebo zamítnutí žádosti o následný certifikát

Žadatel poskytne registrační autoritě elektronickou žádost ve formátu PKCS#10 obsahující veřejný klíč elektronicky způsobem upřesněným na webových stránkách poskytovatele.

Do certifikátu budou vloženy údaje dle platného seznamu žadatelů.

Registrační autorita ověří elektronický podpis na žádosti, zejména platnost certifikátu použitého pro ověření podpisu v době doručení žádosti na Českou poštu (musí být platný), jeho vydávající certifikační autoritu (PostSignum Qualified CA) a zkontroluje ostatní náležitosti žádosti.

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

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

Pokud má registrační autorita pochybnosti o předložené žádosti o následný certifikát nebo pokud se vyskytnou jiné nesrovnalosti, odmítne vydat certifikát a o této skutečnosti informuje žadatele o certifikát.

4.2.3 Doba zpracování žádosti o certifikát

Poskytovatel certifikačních služeb je povinen v nejkratším možném termínu od podání žádosti posoudit žádost o certifikát, vydat rozhodnutí, zda bude certifikát vydán a v případě zamítnutí žádosti o tomto rozhodnutí informovat žadatele o certifikát. Od okamžiku kladného rozhodnutí je poskytovatel povinen neprodleně vydat certifikát.

4.3 Vydání certifikátu

Po kontrole a schválení žádosti o certifikát vloží registrační autorita tuto žádost do systému certifikační autority ke zpracování. Systém certifikační autority na základě této žádosti vydá certifikát a předá ho zpět registrační autoritě a publikačním službám.

Certifikát se stává platným okamžikem vydání.

4.3.1 Úkony CA v průběhu vydávání certifikátu

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

4.3.2 Oznámení o vydání certifikátu držiteli certifikátu nebo podepisující osobě

Na e-mailovou adresu žadatele je odeslána informace o umístění vydaného certifikátu (URL), kde je možné vydaný certifikát po omezenou dobu uvedenou v e-mailové zprávě akceptovat (potvrdit převzetí certifikátu) a certifikát včetně protokolu o vydání certifikátu stáhnout.

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

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

Převzetím certifikátu žadatel o certifikát za zákazníka stvrzuje:

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

- že mu nejsou známy žádné skutečnosti, které by svědčily o tom, že soukromý klíč odpovídající veřejnému klíči v certifikátu vlastní jiná osoba, než je povoleno v příslušné certifikační politice,
- že údaje ve vydaném certifikátu jsou správné a úplné (zejména, že veřejný klíč v certifikátu odpovídá veřejnému klíči uvedenému v poskytnuté PKCS#10 žádosti).

Převzetím certifikátu se zákazník stává držitelem certifikátu.

Vydaný certifikát je podepisující osobě předán ve formátu DER.

4.4.2 Zveřejňování vydaných certifikátů poskytovatelem

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

4.4.3 Oznámení o vydání certifikátu jiným subjektům

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

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, na základě kterých již byl vydán certifikát certifikační autoritou PostSignum Qualified CA, nemohou být v prostředí PostSignum Qualified CA znovu použity.

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

Podepisující osoba:

- nakládá se soukromým klíčem, který odpovídá veřejnému klíči v certifikátu vydaném podle této certifikační politiky, s náležitou péčí, a to tak, aby nemohlo dojít k jeho neoprávněnému použití,
- v případě ztráty, odcizení nebo podezření na kompromitaci soukromého klíče neprodleně informuje poskytovatele certifikačních služeb a zároveň ukončí používání uvedeného soukromého klíče,
- užívá soukromý klíč a odpovídající certifikát vydaný podle této certifikační politiky pouze pro účely stanovené v této certifikační politice, uvedené v kapitole 1.4.1, tj. pro vytváření elektronického podpisu a v souladu s požadavky stanovených platnými právními předpisy,
- v případě, že soukromý klíč je uložen na QESCD, podepisující osoba:
 - o musí mít generování a používání soukromého klíče pod svou výhradní kontrolou,
 - o musí soukromý klíč používat pouze pro vytváření elektronických podpisů a v souladu s platnými právními předpisy.

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

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

- získá certifikáty PostSignum Qualified CA a PostSignum Root QCA z bezpečného zdroje (webové stránky poskytovatele, webové stránky orgánu dohledu, EU Trusted Lists, na pracovišti registrační autority) a ověří otisk ("fingerprint") těchto certifikátů.
- před použitím certifikátu vydaného PostSignum Qualified CA ověří platnost certifikátu PostSignum Qualified CA a následně i platnost vydaného koncového certifikátu; kontrola se provádí na správnost podpisu vydávající autority a vůči příslušnému aktuálnímu CRL a aktuálnímu času, případně pomocí služby OCSP (tuto činnost obvykle vykonává aplikace uživatele certifikátu).
- dostatečně zváží, zda je certifikát vydaný podřízenou certifikační autoritou podle této politiky vhodný pro účel, ke kterému jej chce použít.

4.6 Obnovení certifikátu

Pod službou obnovení certifikátu je myšleno vydání nového certifikátu se stejným veřejným klíčem a novou dobou platnosti. PostSignum 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 nebo podepisující 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 v certifikátu

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

4.7.1 Podmínky pro výměnu dat pro ověřování elektronických podpisů v certifikátu

Vydání následného certifikátu se řídí ustanoveními v kapitole 3.3.1.

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

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

Žádost o vydání následného certifikátu podle této certifikační politiky mohou podat osoby, jimž byl vydán certifikát, o jehož následný certifikát je žádáno.

4.7.3 Zpracování požadavku na výměnu dat pro ověřování elektronických podpisů

Žadatel o následný certifikát požádá o vydání následného certifikátu dle postupů uvedených na webových stránkách poskytovatele.

Zpracování žádosti o následný certifikát se řídí ustanoveními v kapitolách 4.2.1 a 4.2.2.2.

4.7.4 Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických podpisů podepisující osobě

Pro oznámení o vydání následného certifikátu řídí příslušnými ustanoveními kapitoly 4.3.2.

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

Převzetí následného certifikátu se řídí příslušnými ustanoveními kapitoly 4.4.1.

4.7.6 Zveřejňování vydaných certifikátů s vyměněnými daty pro ověřování elektronických podpisů

Zveřejňování následného certifikátu se řídí příslušnými ustanoveními kapitoly 4.4.2.

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

Oznámení o vydání následného certifikátu se řídí příslušnými ustanoveními kapitoly 4.4.3.

4.8 Změna údajů v certifikátu

Certifikát se změněnými údaji lze vydat pouze

- jako nový certifikát podle postupů uvedených v kapitolách 4.1 - 4.4, nebo
- jako následný certifikát podle postupů uvedených v kapitole 4.7, pokud byly změněny pouze údaje, které dovoluje tato certifikační politika změnit v následných certifikátech.

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

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

4.8.1 Podmínky pro změnu údajů v certifikátu

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

V případě, že poskytovatel certifikačních služeb zjistí, že údaje o zákazníkovi nebo žadateli v certifikátu nebo v systému certifikační autority neodpovídají skutečnosti, je oprávněn tyto údaje změnit.

4.8.2 Subjekty oprávněné požadovat změnu údajů v certifikátu

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

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

Pracovník, případně systém registrační autority ověří:

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

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

4.8.4 Oznámení o vydání certifikátu se změněnými údaji podepisující osobě

Totožné s vydáním prvního certifikátu. Viz ustanovení kapitoly 4.3.2.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Totožné s převzetím prvního certifikátu. Viz ustanovení kapitoly 4.4.1.

4.8.6 Zveřejňování vydaných certifikátů se změněnými údaji

Totožné se zveřejněním prvního certifikátu. Viz ustanovení kapitoly 4.4.2.

4.8.7 Oznámení o vydání certifikátu se změněnými údaji jiným subjektům

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

4.9 Zneplatnění a pozastavení platnosti certifikátu

Žádost o zneplatnění certifikátu lze podat níže uvedenými způsoby:

- osobní návštěva registrační autority (pouze v provozní době kontaktního místa)

Seznam kontaktních míst registrační autority je uveden na webových stránkách poskytovatele.

- telefonicky (nonstop)

Telefon: 954 303 303

- e-mailem (nonstop)

E-mail: postsignum@cpost.cz

- webovou aplikací (nonstop)

Webová stránka: www.postsignum.cz/zneplatneni_certifikatu.html

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

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

4.9.1 Podmínky pro zneplatnění certifikátu

Důvody pro zneplatnění certifikátu koncového uživatele jsou především následující:

- jakékoliv podezření na kompromitaci odpovídajícího soukromého klíče,
- ukončení certifikace QESCD v případě, že odpovídající soukromý klíč je na tomto QESCD uložen,
- neplnění podmínek smlouvy o poskytování certifikačních služeb ze strany zákazníka,
- příkaz orgánu dohledu,
- příslušná žádost držitele nebo podepisující osoby,
- další důvody (úmrtí, zánik, zbavení nebo omezení právní způsobilosti podepisující osoby; pozbytí pravdivosti údajů, na jejichž základě byl certifikát vydán).

4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

O zneplatnění certifikátu může požádat:

- zákazník (držitel certifikátu) prostřednictvím pověřené osoby nebo statutárního zástupce, případně osobně (jedná-li se o nepodnikající fyzickou osobu),
- žadatel (podepisující osoba),
- Manažer CA,
- zástupce orgánu dohledu,
- v případě úmrtí nebo obdobných případech, kdy není za sebe podepisující osoba schopna jednat, může o zneplatnění certifikátu požádat prostřednictvím Manažera CA i třetí osoba.

4.9.3 Požadavek na zneplatnění certifikátu

4.9.3.1 Žádost o zneplatnění certifikátu podaná osobně podepisující osobou na registrační autoritě

Žadatel (podepisující osoba) požádá o zneplatnění certifikátu osobně na pracovišti registrační autority, kde prokáže svou totožnost stejným způsobem jako při podávání žádosti o certifikát (viz kapitola 3.2.3). Podepíše písemnou žádost o zneplatnění certifikátu, kterou vytiskne pracovník registrační autority. Žádost obsahuje sériové číslo certifikátu, jméno vydávající certifikační autority a volitelně i důvod zneplatnění.

Pracovník registrační autority vyhledá certifikát a zahájí proces zneplatnění. Ověří, zda žadatel má právo žádat o zneplatnění certifikátu. Pokud ověření proběhne úspěšně, odešle pracovník registrační autority žádost o zneplatnění do systému certifikační autority ke zpracování. Po zpracování žádosti systémem certifikační autority ověří pracovník stav certifikátu a zajistí předání protokolu o zneplatnění certifikátu žadateli.

4.9.3.2 Žádost o zneplatnění certifikátu podaná telefonicky nebo jiným vzdáleným způsobem

Žadatel (podepisující osoba) podává žádost o zneplatnění certifikátu telefonicky na telefonní číslo uvedené v kapitole 4.9, nebo jiným vzdáleným způsobem specifikovaným na webových stránkách poskytovatele. Služba pro telefonické zneplatnění je dostupná 24 hodin denně. Každá takto podaná žádost musí obsahovat sériové číslo certifikátu, jméno vydávající certifikační autority, heslo pro zneplatnění certifikátu a volitelně důvod zneplatnění.

Pracovník oprávněný provádět zneplatnění zkontroluje heslo pro zneplatnění v žádosti oproti heslu zadanému při registraci žádosti o certifikát. V případě, že údaje souhlasí, certifikát zneplatní. V opačném případě pracovník zneplatnění neprovede a informuje žadatele.

Pokud bylo zneplatnění úspěšné, je vytvořen protokol o zneplatnění, který je prostřednictvím elektronické pošty zaslán žadateli na adresu uvedenou ve zneplatněném certifikátu.

4.9.3.3 Žádost o zneplatnění certifikátu podaná pověřenou osobou

V případě, že o zneplatnění žádá zákazník, učiní tak písemnou formou. Pověřená osoba se dostaví osobně na registrační autoritu České pošty, kde s ní bude sepsána žádost o zneplatnění certifikátu.

Pokud pověřená osoba vlastní certifikát určený k podpisu, vydaný podřízenou certifikační autoritou v hierarchii PostSignum, může zaslat žádost o zneplatnění certifikátu v e-mailové zprávě opatřené elektronickým podpisem na adresu uvedenou v kapitole 4.9.

Po úspěšném zneplatnění je vytvořen protokol o zneplatnění certifikátu, který je prostřednictvím elektronické pošty zaslán pověřené osobě. Žadatel je o zneplatnění certifikátu informován prostřednictvím elektronické pošty na kontaktní adresu a na adresu uvedenou ve zneplatněném certifikátu.

4.9.3.4 Zneplatnění certifikátu z vůle certifikační autority

O zneplatnění certifikátu může rozhodnout rovněž poskytovatel certifikačních služeb, pokud podepisující osoba nebo zákazník porušují pravidla certifikační politiky nebo dohodnuté smluvní podmínky. PostSignum QCA v takovém případě informuje zákazníka o zneplatnění certifikátu s udáním důvodu, proč byl certifikát zneplatněn. Manažer CA podává elektronicky podepsanou žádost o zneplatnění certifikátu, kterou předá některému z pracovníků oprávněných provádět zneplatnění certifikátu.

Po úspěšném zneplatnění je vytvořen protokol o zneplatnění certifikátu, který je prostřednictvím elektronické pošty neprodleně zaslán žadateli společně s důvodem zneplatnění certifikátu na kontaktní adresu a na adresu uvedenou ve zneplatněném certifikátu.

4.9.3.5 Zneplatnění certifikátu z vůle orgánu dohledu

O zneplatnění kvalifikovaného certifikátu může rozhodnout rovněž orgán dohledu. PostSignum QCA v takovém případě informuje zákazníka o zneplatnění certifikátu s udáním důvodu, proč byl certifikát zneplatněn. Zástupce orgánu dohledu podává písemnou žádost o zneplatnění certifikátu Manažerovi CA, v žádosti musí být uveden důvod zneplatnění certifikátu.

Po úspěšném zneplatnění je vytvořen protokol o zneplatnění certifikátu, který je prostřednictvím elektronické pošty neprodleně zaslán žadateli společně s důvodem zneplatnění certifikátu na kontaktní adresu a na adresu uvedenou ve zneplatněném certifikátu.

4.9.4 Doba odkladu požadavku na zneplatnění certifikátu

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

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

Doba od přijetí žádosti o zneplatnění certifikátu do zveřejnění CRL obsahujícího i zneplatněný certifikát nepřesáhne 24 hodin.

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

Uživatel certifikátu vydaného PostSignum Qualified CA (spoléhající se strana) je povinen postupovat v souladu s ustanoveními kapitoly 4.5.2.

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů (CRL) je vydáván vždy vzápětí po zpracování žádosti o zneplatnění certifikátu. Nedojde-li ke zneplatnění certifikátu, je nový CRL vydáván alespoň každých 24 hodin (zpravidla každé 4 hodiny). Seznam zneplatněných certifikátů je zveřejňován na těchto místech:

- distribučních bodech CRL (CDP) uvedených v certifikátu
- na webových stránkách poskytovatele,
- u nezávislého poskytovatele webových služeb.

Primárním zdrojem aktuálního CRL jsou distribuční body CRL.

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

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

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

Pro ověření certifikátu vydaného dle této certifikační politiky je možné využít veřejně dostupnou bezplatnou službu OCSP, která je poskytována dle standardu RFC 6960.

Odkaz na OCSP responder je uveden přímo v certifikátu vydaném dle této certifikační politiky, viz profil certifikátu uvedený v kapitole 7.

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

Profil žádosti a odpovědi OCSP responderu je uveden v certifikační prováděcí směrnici.

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

Postup pro zneplatnění certifikátu v případě kompromitace dat pro vytváření elektronických podpisů 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

Status certifikátu je možné ověřit

- na seznamu zneplatněných certifikátů (CRL) v rámci služby umožňující přístup k veřejným informacím PostSignum QCA protokolem HTTP, nebo
- v rámci služby vyhledávání vydaných certifikátů přístupné na webových stránkách poskytovatele, 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 místech uvedených v kapitole 4.9.7.

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

Služba OCSP vrací stav certifikátu v reálném čase (on-line) na základě zaslané žádosti. Informace o stavu certifikátu získané pomocí služby OCSP jsou 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.

Služba OCSP je dostupná 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 nebo podepisující osobu

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

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

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

PostSignum QCA tuto službu neposkytuje.

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

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 zvládnutí 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
- Organizační zajištění úlohy Kvalifikovaná certifikační autorita České pošty, která mj. upravuje 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

5.1.1 Umístění a konstrukce

V PostSignum QCA existují následující typy stabilních pracovišť umístěných v prostorách České pošty nebo jejich smluvních partnerů:

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

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

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

5.1.2 Fyzický přístup

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

5.1.3 Elektřina a klimatizace

Centrální pracoviště jsou připojena na nepřerušitelný zdroj napájení (UPS) a mají nainstalovány 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.

5.1.5 Protipožární opatření a ochrana

Prostory centrálních pracovišť jsou vybaveny elektronickou požární signalizací (EPS).

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 zasílány zálohy systémů PostSignum QCA.

5.2 Procesní bezpečnost

5.2.1 Důvěryhodné role

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

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

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

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

5.2.3 Identifikace a autentizace pro každou roli

Představitel každé role se musí při přístupu k prostředkům PostSignum QCA identifikovat a autentizovat. Každý uživatel má přidělenou jednoznačnou identifikaci ve všech systémech, ke kterým má přístup. V systémech PostSignum QCA je používána identifikace jménem resp. certifikátem a autentizace heslem resp. soukromým klíčem.

5.2.4 Role vyžadující rozdělení povinností

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

5.3 Personální bezpečnost

5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

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

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

5.3.2 Posouzení spolehlivosti osob

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

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

5.3.3 Požadavky na přípravu pro výkon role, vstupní školení

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

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

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

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

5.3.4 Požadavky a periodicita školení

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

Manažer CA v pravidelných intervalech (zejména při změnách v postupech PostSignum QCA) organizuje školení obsluhy.

5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Požadavky na rotaci pracovníků a její frekvenci nejsou definovány.

5.3.6 Postihy za neoprávněné činnosti zaměstnanců

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

5.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

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

5.3.8 Dokumentace poskytovaná zaměstnancům

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

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

5.4 Auditní záznamy (logy)

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

5.4.1 Typy zaznamenávaných událostí

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

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

5.4.2 Periodicita zpracování záznamů

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

5.4.3 Doba uchování auditních záznamů

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

5.4.4 Ochrana auditních záznamů

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

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

5.4.5 Postupy pro zálohování auditních záznamů

Auditní záznamy (kromě auditních záznamů o činnosti centrálních komponent certifikační autority v elektronické podobě) nejsou obecně zálohovány; jsou pouze archivovány. Důležité auditní záznamy spojené s vydáním certifikátů jsou uchovávány ve dvou kopiích, které jsou uloženy v různých lokalitách.

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

V prostředí PostSignum QCA není nasazen systém na centrální shromažďování auditních záznamů. Auditní záznamy jsou shromažďovány v rámci jednotlivých systémů PostSignum QCA.

5.4.7 Postup při oznamování události subjektu, který ji způsobil

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

5.4.8 Hodnocení zranitelnosti

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

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

5.5 Uchovávání informací a dokumentace

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

5.5.1 Typy informací a dokumentace, které se uchovávají

V PostSignum QCA se archivují tyto záznamy:

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

5.5.2 Doba uchování uchovávaných informací a dokumentace

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

5.5.3 Ochrana úložiště uchovávaných informací a dokumentace

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

5.5.4 Postupy při zálohování uchovávaných informací a dokumentace

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

5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

Pokud jsou v PostSignum QCA využívána časová razítka, jedná se o kvalifikovaná elektronická časová razítka PostSignum QCA.

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

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

5.5.7 Postupy pro získání a ověření uchovávaných informací a dokumentace

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

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

Přístup k archivům je omezen na osoby v odpovídajících rolích.

5.6 Výměna dat pro ověřování elektronických pečeti v nadřazeném certifikátu pro elektronickou pečeť poskytovatele

Platnost klíčů certifikačních autorit v hierarchii PostSignum QCA je omezena.

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

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

Plánovaná výměna klíčů certifikační autority musí být oznámena zákazníkům nejpozději 3 měsíce před aktivním používáním nového certifikátu PostSignum Root QCA resp. 1 měsíc před aktivním používáním certifikátu autority PostSignum Qualified CA. Toto oznámení bude (včetně důvodu ukončení platnosti certifikátu) zveřejněno na webových stránkách poskytovatele a na všech pracovištích registrační autority PostSignum QCA.

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

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

5.7 Obnova po havárii nebo kompromitaci

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

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

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

5.7.1 Postup v případě incidentu a kompromitace

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

5.7.2 Poškození výpočetních prostředků, softwaru nebo dat

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

5.7.3 Postup při kompromitaci dat pro vytváření elektronických pečeti poskytovatele

5.7.3.1 Kompromitace soukromého klíče podřízené certifikační autority

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

PostSignum Root QCA okamžitě zneplatní certifikát PostSignum Qualified CA a tato zneplatní všechny platné certifikáty vydané koncovým zákazníkům; zneplatněné certifikáty budou neprodleně zveřejněny na příslušném CRL.

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

Česká pošta prokazatelně zničí data pro vytváření elektronických pečeti. PostSignum Qualified CA, která sloužila pro pečetení kvalifikovaných certifikátů a seznamů zneplatněných certifikátů, u nichž existuje podezření na kompromitaci, a o tomto zničení provede záznam.

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

5.7.3.2 Kompromitace soukromého klíče PostSignum Root QCA

V případě podezření na kompromitaci soukromého klíče PostSignum Root QCA provede poskytovatel certifikačních služeb zneplatnění certifikátu PostSignum Root QCA, platných certifikátů všech podřízených certifikačních autorit a všech jimi vydaných platných certifikátů; zneplatněné certifikáty budou neprodleně zveřejněny na příslušném CRL. O zneplatnění certifikátů (případně o mimořádném ukončení činnosti autority) budou písemně nebo elektronicky informováni všichni držitelé certifikátů, orgán dohledu a subjekty, které mají uzavřenou smlouvu přímo se vztahující k poskytování certifikačních služeb; oznámení

bude rovněž zveřejněno na webových stránkách poskytovatele, na všech pracovištích registrační autority PostSignum QCA a v jednom celostátně vydávaném deníku. Součástí oznámení bude i důvod ukončení platnosti certifikátu certifikační autority.

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

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

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

5.7.4 Schopnost obnovit činnost po havárii

Obnova činnosti po havárii se řídí platným interním dokumentem Plán zvládnání krizových situací a plán obnovy.

5.8 Ukončení činnosti CA nebo RA

5.8.1 Ukončení činnosti kořenové certifikační autority

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

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

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

Následně ČP prokazatelně zničí data pro vytváření elektronických pečeti PostSignum Root QCA, která sloužila pro pečetení kvalifikovaných certifikátů a seznamů zneplatněných certifikátů, a o tomto zničení provede záznam. Záznamy budou uchovávány v souladu s ustanoveními této certifikační politiky uvedenými v kapitole 5.4.

5.8.2 Ukončení činnosti podřízené certifikační autority

Ukončení činnosti PostSignum Qualified CA musí být písemně oznámeno všem držitelům platných certifikátů, orgánu dohledu a subjektům, které mají uzavřenou smlouvu přímo se vztahující k poskytování certifikačních služeb a rovněž zveřejněno na webových stránkách poskytovatele a na všech pracovištích registrační autority PostSignum QCA. Součástí oznámení musí být i informace o ukončení platnosti certifikátu autority včetně příslušného důvodu ukončení. Dokud je platný alespoň jeden certifikát vydaný PostSignum Qualified CA, musí tato autorita zajišťovat alespoň funkci zneplatnění certifikátu a vydání CRL.

Pokud PostSignum Qualified CA tuto funkci není schopna zajistit po celou dobu platnosti vydaných certifikátů, musí o této skutečnosti informovat držitele platných certifikátů spolu s uvedením data, do kdy bude funkce poskytována. Toto datum může být nejdříve 3 měsíce ode dne zaslání oznámení. K tomuto datu PostSignum Qualified CA zneplatní všechny dosud platné vydané certifikáty a vydá poslední CRL. Teprve poté může být činnost této autority ukončena.

Zneplatněný certifikát pro elektronickou pečeť PostSignum Qualified CA bude zveřejněn na CRL PostSignum Root QCA v čase uvedeném v certifikační politice PostSignum Root QCA.

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

Následně ČP prokazatelně zničí data pro vytváření elektronických pečeti PostSignum Qualified CA, která sloužila pro pečetení kvalifikovaných certifikátů a seznamů zneplatněných certifikátů, a o tomto zničení provede záznam. Záznamy budou uchovávány v souladu s ustanoveními této certifikační politiky uvedenými v kapitole 5.4.

5.8.3 Ukončení činnosti registrační autority

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

5.8.4 Ukončení činnosti poskytovatele certifikačních služeb

Činnost poskytovatele certifikačních služeb bude ukončena v souladu s platnými právními předpisy. Pokud po ukončení činnosti poskytovatele certifikačních služeb nebude nadále možné zajistit přístup k údajům, které byly evidovány z důvodu poskytování certifikačních služeb, a které by mohly sloužit pro účely poskytnutí důkazů v soudním a správním řízení a pro účely zajištění kontinuity služby, tak tyto údaje předá Manažer CA orgánu dohledu.

5.8.5 Odnětí akreditace

V případě odnětí akreditace musí být informace o odnětí akreditace písemně nebo elektronicky oznámena všem držitelům platných certifikátů a subjektům, které mají uzavřenou smlouvu přímo se vztahující k poskytování certifikačních služeb a zveřejněna na webových stránkách poskytovatele, na všech pracovištích registrační autority PostSignum QCA a dalšími způsoby uvedenými v platných právních předpisech. Součástí informace bude i sdělení, že kvalifikované certifikáty vydané tímto poskytovatelem nelze nadále používat podle platných právních předpisů.

O dalším postupu v tomto případě rozhodne management ČP na základě příslušného rozhodnutí orgánu dohledu.

6 TECHNICKÁ BEZPEČNOST

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Klíčové páry certifikačních autorit v hierarchii PostSignum QCA jsou generovány a uloženy v hardwarovém kryptografickém modulu. Generování těchto klíčových párů probíhá kontrolovaným procesem, na jehož průběh dohlíží Manažer CA a Auditor CA.

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

Klíčové páry operátorů PostSignum QCA (včetně operátorů RA; kontrolní klíče) jsou generovány ve vyhrazených hardwarových prostředcích, které svou konstrukcí neumožňují export soukromých klíčů. Pro použití soukromých klíčů je vždy nutné zadat PIN.

Soukromé klíče žadatelů jsou generovány a uschovávány žadatelem o certifikát. Klíče mohou být generovány a následně i uloženy jak v softwarovém, tak i hardwarovém úložišti. PostSignum QCA nepředepisuje konkrétní požadavky na příslušné úložiště.

Pokud žadatel požaduje vydání certifikátu s příznakem, že soukromý klíč je uložený na QESCD, musí být soukromý klíč vygenerován přímo na QESCD.

6.1.2 Předání dat pro vytváření elektronických podpisů podepisující osobě

PostSignum QCA neposkytuje službu generování klíčových párů pro žadatele o certifikát a se soukromými klíči žadatelů nepřichází do styku a není zodpovědná za jejich ochranu ani zálohování.

V případě, že poskytovatel spravuje a provozuje QESCD pro účely uložení dat pro vytváření elektronických podpisů žadatelem zákazníka, generování soukromého klíče provádí poskytovatel přímo v QESCD dle podmínek dohodnutých se zákazníkem.

6.1.3 Předání dat pro ověřování elektronických podpisů 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 pečeti certifikační autoritou spoléhajícím se stranám

Certifikáty certifikačních autorit a dále certifikáty podepisujících nebo pečetičících osob, pro které byl vysloven souhlas se zveřejněním, jsou zveřejněny způsobem popsáným v kapitole 2.

6.1.5 Délky párových dat

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

Klíče držitelů certifikátů mají pro algoritmus RSA délku modulu 2048 nebo 4096 bitů. Jiný algoritmus než RSA není pro držitele certifikátů povolen.

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

Parametry používané při vytváření veřejných klíčů komponent PostSignum QCA jsou generovány odpovídajícím softwarovým a hardwarovým vybavením. Použité algoritmy a jejich parametry odpovídají požadavkům platných právních předpisů nebo technických norem, které upravují činnost poskytovatelů certifikačních služeb.

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

Kontrola kvality dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických pečetí je nastavena na úrovni certifikační autority, která kontroluje jedinečnost a povolenou délku veřejného klíče.

6.1.7 Omezení pro použití dat pro ověřování elektronických podpisů

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, dat pro vytváření elektronických značek nebo dat pro ověřování elektronických pečetí a bezpečnost kryptografických modulů

6.2.1 Standardy a podmínky používání kryptografických modulů

Kryptografický modul použitý pro generování a úschovu soukromého klíče certifikačních autorit (nástroj pro vytváření elektronického podpisu nebo elektronické pečetě) působících v hierarchii PostSignum QCA splňuje požadavky standardu FIPS 140-2 Level 3 a byla mu orgánem dohledu vyslovena shoda.

6.2.2 Sdílení tajemství

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

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

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

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

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

Soukromý klíč certifikační autority je zálohován v zašifrované formě. Při obnově zálohovaných klíčů do nového nebo inicializovaného modulu je zapotřebí součinnosti minimálně tří osob.

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

Soukromé klíče certifikačních autorit v hierarchii PostSignum QCA nejsou archivovány. Po ukončení provozu certifikační autority jsou klíče včetně záloh zničeny, o čemž je vyhotoven záznam.

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

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

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

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

6.2.7 Uložení dat pro vytváření elektronických pečeti v kryptografickém modulu

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

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

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

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

6.2.9 Postup při deaktivaci dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečeti

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

6.2.10 Postup při zničení dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečeti

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

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

6.2.11 Hodnocení kryptografických modulů

Vzhledem ke skutečnosti, že kryptografický modul užívaný k úschově soukromého klíče certifikační autority úspěšně prošel hodnocením podle standardu FIPS 140–2 na úroveň 3, nepředpokládá se, že by obsahoval

závažné chyby na úrovni konstrukce zařízení. Přesto se průběžně sleduje, zda nebyl objeven útok na toto zařízení, aby bylo možné včas na takové ohrožení reagovat.

6.3 Další aspekty správy párových dat

6.3.1 Uchovávání dat pro ověřování elektronických podpisů

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

6.3.2 Maximální doba platnosti certifikátu vydaného podepisující osobě a párových dat

Délka platnosti certifikátu je 385 dní nebo 1115 dní dle objednávky zákazníka. Při vydání nového certifikátu v rámci reklamačního řízení nebo na žádost zákazníka při změně údajů, může být doba platnosti certifikátu zkrácena.

Doba platnosti certifikátu vydaného podle této certifikační politiky je vždy uvedena v certifikátu.

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 interních dokumentech Systémové bezpečnostní politika, Provozní a bezpečnostní procedury a v interní provozní dokumentaci.

6.4.1 Generování a instalace aktivačních dat

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

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

6.4.2 Ochrana aktivačních dat

Všechna aktivační data musí být chráněna před prozračením neoprávněné osobě. Příslušné povinnosti v tomto smyslu mají všichni pracovníci PostSignum QCA a jsou uvedeny v interním dokumentu Systémová bezpečnostní politika.

6.4.3 Ostatní aspekty aktivačních dat

Ostatní aspekty týkající se aktivačních dat, jejich generování, instalace a používání, jsou popsány v interních dokumentech Systémové bezpečnostní politika, Provozní a bezpečnostní procedury a v interní provozní dokumentaci.

6.5 Počítačová bezpečnost

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Pro každou komponentu v hierarchii PostSignum QCA jsou definována nastavení zajišťující bezpečnost dané komponenty na technologické úrovni, které vycházejí z požadavků platných právních předpisů a návazných dokumentů, a to zejména ze standardů [ETSI EN 319 401] a [ETSI EN 319 411].

6.5.2 Hodnocení počítačové bezpečnosti

System PostSignum QCA prošel po vybudování externí kontrolou bezpečnostní shody zaměřenou na splnění požadavků kladených legislativou na kvalifikovaného poskytovatele služeb vytvářejících důvěru, a to zejména požadavků uvedených v [eIDAS].

6.6 Bezpečnost životního cyklu

6.6.1 Řízení vývoje systému

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

Následné změny jsou realizovány v souladu s definovaným změnovým řízením.

6.6.2 Kontroly řízení bezpečnosti

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

6.6.3 Řízení bezpečnosti životního cyklu

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

6.7 Síťová bezpečnost

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

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

Veškerá komunikace mimo vyhrazené lokální sítě centrálních pracovišť je šifrovaná.

6.8 Časová razítka

Viz kapitola 5.5.5.

7 PROFILY CERTIFIKÁTU, SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ A OCSP

7.1 Profil certifikátu

PostSignum QCA vydává certifikáty odpovídající standardu X.509. Profil kvalifikovaného certifikátu pro elektronický podpis je uveden v následující tabulce. Certifikační autorita si vyhrazuje právo vložit do certifikátu další položky, pokud si to vyžádá změna právních předpisů nebo technických norem, které upravují činnost poskytovatelů certifikačních služeb.

Tab. 2 Profil kvalifikovaného certifikátu pro elektronický podpis

Položka	Hodnota	Pov.	Změna	ORG	PFO	NFO
Version	3 (0x2)	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.				
Serial number	sériové číslo certifikátu přidělené certifikační autoritou					
SignatureAlgorithm	sha256WithRSA nebo sha256WithRSASSA-PSS					
Issuer						
C countryName	CZ	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit. (X je číslo označující konkrétní podřízenou certifikační autoritu)				
OID 2.5.4.97 organizationIdentifier	NTRCZ-47114983					
O organisationName	Česká pošta, s.p.					
CN commonName	PostSignum Qualified CA X					
Validity						
Not Before	Počátek platnosti vydaného certifikátu (UTCTime)	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit. Délka platnosti certifikátů je uvedena v kapitole 6.3.2.				
Not After	Konec platnosti vydaného certifikátu (UTCTime)					
Subject						
C countryName	kód státu, kde má zákazník (právnícká osoba) sídlo, fyzická nepodnikající osoba bude mít uveden vždy kód CZ	ano	ne	X	X	X
L localityName	trvalé bydliště / kontaktní adresa fyzické osoby	ne	ano			X
OID 2.5.4.97 organizationIdentifier	obsahuje identifikátor organizace dle mezinárodních standardů ve tvaru: NTRYY- <i>IČO</i> organizace nebo VATYY- <i>DIČ</i> organizace <i>YY je kód státu, kde má zákazník sídlo</i>	ano	ano	X	X	
O organisationName	jméno právnické osoby nebo podnikající fyzické osoby	ano	ano	X	X	
OU organizationalUnitName	rozdílní organizací jednotka právnické osoby nebo podnikající fyzické osoby	ne	ano	X	X	
OU organizationalUnitName	organizační jednotka	ne	ano	X	X	
OU organizationalUnitName	číslo žadatele o certifikát v prostředí zákazníka – organizace nebo podnikající fyzické osoby	ano	ano	X	X	
CN commonName	jméno a příjmení osoby (včetně případných titulů) * změna titulů v následném certifikátu je možná	ano	ne*	X	X	X

SN surname	příjmení osoby	ano	ne	X	X	X
givenName	křestní jméno osoby	ano	ne	X	X	X
serialNumber	jednoznačný identifikátor osoby, přidělovaný poskytovatelem certifikačních služeb ve tvaru: <i>Pčíslo</i>	ano	ne	X	X	X
title	funkce žadatele o certifikát	ne	ano	X	X	
Subject Public Key Info						
Algorithm	rsaEncryption	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.				
SubjectPublicKey	veřejný klíč podepisující osoby o velikosti 2048 nebo 4096 bitů					
Extensions	rozšíření certifikátu podle tabulky 3					
Signature	elektronická pečeť poskytovatele certifikačních služeb					

Vysvětlivky:

Pov povinná položka certifikátu

Změna položku je možné změnit v následném certifikátu

ORG položka je obsažena v certifikátech vydávaných zaměstnancům organizací

PFO položka je obsažena v certifikátech vydávaných podnikajícím fyzickým osobám

NFO položka je obsažena v certifikátech vydávaných nepodnikajícím fyzickým osobám

7.1.1 Číslo verze

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

7.1.2 Rozšiřující položky v certifikátu

Rozšiřující položky použité v kvalifikovaném certifikátu pro el. podpis jsou uvedeny v následující tabulce.

Tab. 3 Rozšíření v certifikátu

Položka	Hodnota	Pov.	Změna	ORG	PFO	NFO
Authority Key Identifier						
Key Identifier		Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.				
Subject Key Identifier						
Subject Alternative Name						
rfc822Name emailAddress	e-mailová adresa žadatele	ano	ano	X	X	X
rfc822Name emailAddress	e-mailová adresa žadatele	ne	ano	X	X	X
rfc822Name emailAddress	e-mailová adresa žadatele	ne	ano	X	X	X
otherName	identifikátor MPSV OID položky je: 1.3.6.1.4.1.11801.2.1	ne	ano	X	X	X
otherName	vlastní obsah určený zákazníkem, obsah je kódován pomocí ASCII v hexadecimálním zápisu, položka „Description“ s OID: 2.5.4.13	ne	ano	X	X	X
Key Usage (kritické rozšíření)						
DigitalSignature	ano/ne*	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.				
NonRepudiation	ano					
KeyEncipherment	ano/ne*					
DataEncipherment	ne					
KeyAgreement	ne					

KeyCertSign	ne	* Pokud je odpovídající soukromý klíč uložený na QESCD, nejsou položky označené * uvedené v Key Usage.
CRLSign	ne	
Extended Key usage		
Secure E-mail	id-kp-emailProtection OID 1.3.6.1.5.5.7.3.4	Rozšířené použití klíče je uvedeno ve všech vydávaných certifikátech a nelze je změnit.
Document Signing	id-ms-kp-document-signing OID 1.3.6.1.4.1.311.10.3.12	
Certificate Policies		
Policy Information [1]		
Policy Identifier	OID této certifikační politiky	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.
Policy Qualifier id	CPS	
CPS URI	http://www.postsignum.cz	
User Notice	Tento kvalifikovaný certifikát pro elektronicky podpis byl vydán v souladu s nařízením EU č. 910/2014. This is a qualified certificate for electronic signature according to Regulation (EU) No 910/2014.	
Policy Information [2]		
Policy Identifier	OID pro QCP-n: 0.4.0.194112.1.0 nebo OID pro QCP-n-qscd: 0.4.0.194112.1.2	Povinně je uvedeno vždy jedno z OID. OID 0.4.0.194112.1.2 je uvedeno pouze, pokud je odpovídající soukromý klíč uložený na QESCD.
Qualified certificate statement		
OID	0.4.0.1862.1.1 <i>esi4-QCStatement-1</i>	Položka je obsažena povinně ve všech vydávaných certifikátech a nelze ji změnit.
OID	0.4.0.1862.1.4 <i>esi4-QCStatement-4</i>	Je uvedeno pouze, pokud je odpovídající soukromý klíč uložený na QESCD.
OID	0.4.0.1862.1.5 <i>esi4-QCStatement-5</i>	Položka je obsažena povinně ve všech vydávaných certifikátech a nelze ji změnit. Hodnotou položky je odkaz na zprávu pro uživatele v anglické a české verzi.
OID	0.4.0.1862.1.6.1 <i>esi4-QCStatement-6</i> <i>(id-etsi-qct-esign)</i>	Položka je obsažena povinně ve všech vydávaných certifikátech a nelze ji změnit. Položka značí, že certifikát byl vydán jako kvalifikovaný certifikát pro elektronický podpis dle [eIDAS].
CRL Distribution Points		
URI	http://crl.postsignum.cz/crl/psqualifiedcaX.crl	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit. <i>(X je číslo označující konkrétní podřízenou certifikační autoritu)</i>
URI	http://crl2.postsignum.cz/crl/psqualifiedcaX.crl	
URI	http://crl.postsignum.eu/crl/psqualifiedcaX.crl	
AuthorityInfoAccess		
accessMethod	id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.
URI	http://crt.postsignum.cz/crt/psqualifiedcaX.crt	

accessMethod	id-ad-ocsp (1.3.6.1.5.5.7.48.1)	(X je číslo označující konkrétní podřízenou certifikační autoritu)
URI	http://ocsp.postsignum.cz/OCSP/QCAX/	

Vysvětlivky:

Pov povinná položka certifikátu

Změna položku je možné změnit v následném certifikátu

ORG položka je obsažena v certifikátech vydávaných zaměstnancům organizací

PFO položka je obsažena v certifikátech vydávaných podnikajícím fyzickým osobám

NFO položka je obsažena v certifikátech vydávaných nepodnikajícím fyzickým osobám

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

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

7.1.3 Objektové identifikátory (dále „OID“) algoritmů

Algoritmům používaným v PostSignum 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 právních předpisů a technických norem, které upravují činnost poskytovatelů certifikačních služeb.

7.1.4 Způsoby zápisu jmen a názvů

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

7.1.5 Omezení jmen a názvů

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

7.1.6 OID certifikační politiky

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

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, textovou informaci o skutečnosti, že certifikát byl vydán jako kvalifikovaný certifikát pro elektronický podpis podle [eIDAS] a další položky odpovídající technickým standardům pro kvalifikované certifikáty, které jsou v souladu s [eIDAS].

7.1.9 Způsob zápisu kritické rozšiřující položky „Certificate Policies“

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

7.2 Profil seznamu zneplatněných certifikátů

Tab. 4 Profil CRL

Název položky	Hodnota/příznak použití
Version	2 (0x1)
Issuer Distinguished Name	
C countryName	CZ
OID 2.5.4.97 organizationIdentifier	NTRCZ-47114983
O organisationName	Česká pošta, s.p.
CN commonName	PostSignum Qualified CA X (X je číslo označující konkrétní podřízenou certifikační autoritu)
Validity	
This Update	Počátek platnosti vydaného CRL (UTCTime)
Next Update	Konec platnosti vydaného CRL (UTCTime)
RevokedCertificates	opakující se položka pro každý zneplatněný certifikát
UserCertificate	sériové číslo zneplatněného certifikátu
RevocationDate	datum a čas zneplatnění
CrlEntryExtensions	rozšíření položky CRL podle tabulky 5
CrlExtensions	rozšíření CRL podle tabulky 5
SignatureAlgorithm	sha256WithRSAEncryption
Signature	elektronická pečeť poskytovatele certifikačních služeb

7.2.1 Číslo verze

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

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

Tab. 5 Rozšíření v CRL

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

7.3 Profil OCSP

Viz ustanovení v kapitole 4.9.9.

7.3.1 Číslo verze

Viz ustanovení v kapitole 4.9.9.

7.3.2 Rozšiřující položky OCSP

Viz ustanovení v kapitole 4.9.9.

8 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

V prostředí PostSignum QCA jsou pravidelně prováděny interní kontroly (jednou za 12 měsíců). Kromě těchto interních kontrol jsou prováděny externí kontroly dle platných právních předpisů. Tyto pravidelné kontroly mohou být podle potřeby doplněny další kontrolou, mimo jiné na základě rozhodnutí Manažera CA, managementu České pošty nebo interního auditu České pošty.

8.2 Identita a kvalifikace hodnotitele

Interní kontrolu provádějí pracovníci znalí problematiky PKI a proškolení pro daný úkol. Pracovníci provádějící kontrolu jsou v dokumentaci QCA označováni jako Auditoři CA.

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

8.3 Vztah hodnotitele k hodnocenému subjektu

Interní kontrolu provádí zaměstnanci České pošty, kteří se nepodílejí na provozu certifikační autority PostSignum QCA.

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

8.4 Hodnocené oblasti

Oblasti hodnocené v rámci pravidelných kontrol jsou specifikovány v platných právních předpisech a příslušnými standardy.

8.5 Postup v případě zjištění nedostatků

Výsledky kontrol jsou předávány Manažerovi CA, který zajistí nápravu zjištěných nedostatků.

V případě zjištění nedostatků, které závažně ovlivní schopnost PostSignum QCA dostát svým závazkům a požadavkům uvedeným v platných právních předpisech, přeruší PostSignum QCA vydávání certifikátů do doby, než budou nedostatky odstraněny.

8.6 Sdělování výsledků hodnocení

O provedení každé kontroly je vypracována podepsaná písemná zpráva, která je předána Manažerovi CA. Ten zajistí její distribuci a projednání. Pokud je to nutné, zajistí Manažer CA předání zprávy orgánu dohledu do termínu, který je stanoven platným právním předpisem.

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

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

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

9.1.2 Poplatky za přístup k certifikátu na seznamu vydaných certifikátů

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

9.1.3 Poplatky za informace o statutu certifikátu nebo o zneplatnění certifikátu

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

9.1.4 Poplatky za další služby

Cena za další služby PostSignum QCA je stanovena v ceníku služeb České pošty.

9.1.5 Jiná ustanovení týkající se poplatků (vč. refundací)

Žádná ustanovení v této kapitole.

9.2 Finanční odpovědnost

9.2.1 Krytí pojištěním

Česká pošta má sjednané pojištění odpovědnosti za škodu takovým způsobem, aby byly pokryty případné škody.

9.2.2 Další aktiva a záruky

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

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

9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

PostSignum QCA tuto službu neposkytuje.

9.3 Citlivost obchodních informací

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

9.3.1 Výčet citlivých informací

Za důvěrné jsou považovány všechny informace s výjimkou informací uvedených v dokumentech s označením „Veřejné“.

9.3.2 Informace mimo rámec citlivých informací

Za důvěrné se nepovažují informace, které:

- se staly veřejně známými, aniž by to zavinila záměrně či opomenutím přijímající strana,
- měla přijímající strana legálně k dispozici před uzavřením smlouvy o poskytování certifikačních služeb, pokud takové informace nebyly předmětem jiné, dříve mezi zúčastněnými stranami uzavřené smlouvy o ochraně informací, nebo pokud takové informace nemají samy o sobě charakter obchodního tajemství,
- jsou výsledkem postupu, při kterém k nim přijímající strana dospěje nezávisle a je schopna to doložit svými záznamy nebo důvěrnými informacemi třetí strany,
- po uzavření smlouvy o poskytování certifikačních služeb poskytne přijímající straně třetí osoba, jež takové informace přitom nezíská přímo ani nepřímo od strany, jež je jejich vlastníkem, nebo je nezíská nezákonným způsobem, o čemž by přijímající strana věděla nebo vědět musela,
- jsou uvedené v kvalifikovaném certifikátu, pokud k jeho zveřejnění dal držitel souhlas.

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.

9.3.4 Poskytnutí citlivých informací pro soudní či správní účely

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

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 ve Všeobecných obchodních podmínkách certifikačních služeb a vycházejí z [GDPR].

9.4.1 Osobní údaje

Za osobní údaje jsou považovány veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat.

9.4.2 Odpovědnost za ochranu osobních údajů

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

9.4.3 Poskytnutí osobních údajů

V této oblasti je postupováno podle příslušných ustanovení [GDPR], obecně závazných právních předpisů a interních předpisů České pošty upravujících problematiku ochrany osobních údajů.

9.5 Práva duševního vlastnictví

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

9.6 Zastupování a záruky

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

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

9.6.1 Zastupování a záruky CA

Viz ustanovení kapitoly 9.6.

9.6.2 Zastupování a záruky RA

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.

Jinak viz ustanovení kapitoly 9.6.

9.6.3 Zastupování a záruky držitele certifikátu nebo podepisující osoby

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

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 této certifikační politice, především v kapitole 4.5.2.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

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

Záruky, které v těchto případech poskytuje poskytovatel certifikačních služeb, jsou definovány příslušnými ustanoveními v platných právních předpisech.

9.7 Zřeknutí se záruk

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

Česká pošta neodpovídá za vady poskytnutých služeb vzniklé z důvodu nesprávného nebo neoprávněného využívání služeb poskytnutých v rámci plnění smlouvy o poskytování certifikačních služeb držitelem, zejména za provozování v rozporu s podmínkami uvedenými v této certifikační politice, jakož i za vady vzniklé z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení aj.

9.8 Omezení odpovědnosti

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

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

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

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

9.9 Odpovědnost za škodu, náhrada škody

Pokud nevyplývá z ustanovení platných právních předpisů jinak, odpovídá Česká pošta držiteli certifikátu za škodu způsobenou porušením povinností České pošty v souvislosti s plněním smlouvy o poskytování certifikačních služeb.

9.10 Doba platnosti, ukončení platnosti

9.10.1 Doba platnosti

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

9.10.2 Ukončení platnosti

Platnost dokumentu je ukončena v případě

- jeho nahrazení novější verzí, nebo
- ukončení poskytování služeb Českou poštou jako poskytovatelem certifikačních služeb.

9.10.3 Důsledky ukončení a přetrvání závazků

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

9.11 Komunikace mezi zúčastněnými subjekty

9.11.1 Komunikace s poskytovatelem certifikačních služeb

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

certifikačních služeb opět na webových stránkách a současně písemným nebo elektronickým upozorněním směřovaným na zákazníky.

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

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

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

9.11.2 Komunikace v rámci systému PostSignum QCA

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

9.11.3 Komunikační jazyk

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

9.12 Změny

9.12.1 Postup při změnách

Postupy pro zapracování změn jsou uvedeny v kapitole 1.5.

9.12.2 Postup při oznamování změn

Vydání nové certifikační politiky se změněným OID (viz následující kapitola) bude oznámeno v aktualitách na webových stránkách poskytovatele.

V případě identifikace oslabení záruk poskytovaných používanými kryptografickými algoritmy vyžadující neodkladný zásah budou písemně nebo elektronicky informováni všichni držitelé certifikátů, orgán dohledu a subjekty, které mají uzavřenou smlouvu přímo se vztahující k poskytování certifikačních služeb. Oznámení bude rovněž zveřejněno na webových stránkách poskytovatele, na všech pracovištích registrační autority PostSignum QCA. Na toto oznámení mohou navazovat další akce, které jsou popsány v této certifikační politice.

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

9.12.3 Okolnosti, při kterých musí být změněn OID

Česká pošta 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 certifikační prováděcí směrnicí.

Pouze větší změna v certifikační politice vyvolá změnu verze dokumentu na úrovni **x.x** a také změnu OID. Menší změny vyvolají změnu verze dokumentu na úrovni **x.x.x**, přičemž OID se nemění.

9.13 Řešení sporů

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

- Manažera CA, nebo
- registrační autoritu (formou žádosti o reklamaci).

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

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 politiky 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

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

V případě ukončení činnosti kvalifikovaného poskytovatele certifikačních služeb vyvine Česká pošta v souladu s platnými právními předpisy přiměřené úsilí pro převzetí správy platných kvalifikovaných certifikátů a související agendy jiným kvalifikovaným poskytovatelem certifikačních služeb. V tomto případě budou vztahy mezi tímto kvalifikovaným poskytovatelem certifikačních služeb a Českou poštou rovněž upraveny zvláštní smlouvou.

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

9.16.3 Oddělitelnost ustanovení

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

9.16.4 Zřeknutí se práv

Žádná ustanovení v této kapitole.

9.16.5 Vyšší moc

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

9.16.6 Přístupnost pro osoby se zdravotním postižením

Poskytované služby vytvářející důvěru a konečné uživatelské produkty používané při poskytování těchto služeb jsou dostupné osobám se zdravotním postižením. Bližší informace ohledně poskytování služeb těmto osobám poskytnou registrační autority nebo Zákaznická podpora. Kontaktní údaje jsou uvedené na webových stránkách poskytovatele www.postsignum.cz.

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/ES |
| [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 |
| [GDPR] | NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) |
| [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
- [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