Certifikační politika PostSignum Public CA pro komerční doménové certifikáty

Verze 5.1.0

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

OBSAH

1 Úvod 4
1.1 Přehled 4
1.2 Název a jednoznačné určení dokumentu 4
1.3 Participující subjekty 6
1.4 Použití certifikátu 7
1.5 Správa politiky 7
1.6 Přehled použitých pojmů a zkratek 7

2 Odpovědnost za zveřejňování a úložiště informací a dokumentace 11
2.1 Úložiště informací a dokumentace 11
2.2 Zveřejňování informací a dokumentace 11
2.3 Periodicita zveřejňování informací 12
2.4 Řízení přístupu a úložiště 12

3 Identifikace a autentizace 13
3.1 Pojmenování 13
3.2 Počáteční ověření identity 14
3.3 Identifikace a autentizace při zpracování požadavků na výměnu veřejného klíče v certifikátu 16
3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu 16

4 Požadavky na životní cyklus certifikátu 17
4.1 Žádost o vydání certifikátu 17
4.2 Zpracování žádosti o certifikát 19
4.3 Vydání certifikátu 20
4.4 Převzetí vydaného certifikátu 20
4.5 Použití párových dat a certifikátu 21
4.6 Obnovení certifikátu 22
4.7 Výměna veřejného klíče v certifikátu 22
4.8 Změna údajů v certifikátu 22
4.9 Zneplatnění a pozastavení platnosti certifikátu 23
4.10 Služby související s ověřováním stavu certifikátu 28
4.11 Ukončení poskytování služeb pro držitele certifikátu 29
4.12 Úschova soukromého klíče u důvěryhodné třetí strany a jejich obnova 29

5 Management, provozní a fyzická bezpečnost 30
5.1 Fyzická bezpečnost 30
5.2 Procesní bezpečnost 31
5.3 Personální bezpečnost 32
5.4 Auditní záznamy (logy) 33
5.5 Uchovávání informací a dokumentace 35
5.6 Výměna veřejného klíče elektronických pečetí v nadřízeném certifikátu pro elektronickou pečeť poskytovatele 35
5.7 Obnova po havárii nebo kompromitaci 36
5.8 Ukončení činnosti CA nebo RA 38

6 Technická bezpečnost 40
6.1 Generování a instalace párových dat 40

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

6.2 Ochrana soukromého klíče a bezpečnost kryptografických modulů 41
6.3 Další aspekty správy párových dat....43
6.4 Aktivační data 43
6.5 Počítačová bezpečnost 44
6.6 Bezpečnost životního cyklu 44
6.7 Síťová bezpečnost 44
6.8 Časová razítka 45

7 Profily certifikátu, seznamu zneplatněných certifikátů a OCSP 46
7.1 Profil certifikátu 46
7.2 Profil seznamu zneplatněných certifikátů 53
7.3 Profil OCSP 54

8 Hodnocení shody a jiná hodnocení 56
8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení 56
8.2 Identita a kvalifikace auditora 56
8.3 Vztah hodnotitele k hodnocenému subjektu 56
8.4 Hodnocené oblasti 56
8.5 Audit se provádí v souladu s normami [ETSI EN 319 401], [ETSI EN 319 411] (měla by být použita nejnovější verze odkazovaných dokumentů ETSI), část 1 – 3 v souladu s požadavky Mozilla a [CA/B] v aktuální verzi požadavků CCADB.Postup v případě zjištění nedostatků 56
8.6 Sdělování výsledků hodnocení....57
8.7 Vlastní audity 57

9 Ostatní obchodní a právní záležitosti 58
9.1 Poplatky 58
9.2 Finanční odpovědnost 58
9.3 Citlivost obchodních informací....58
9.4 Ochrana osobních údajů....59
9.5 Práva duševního vlastnictví 60
9.6 Zastupování a záruky 60
9.7 Zřeknutí se záruk....60
9.8 Omezení odpovědnosti....61
9.9 Odpovědnost za škodu, náhrada škody 61
9.10 Doba platnosti, ukončení platnosti....61
9.11 Komunikace mezi zúčastněnými subjekty 61
9.12 Změny 62
9.13 Řešení sporů....63
9.14 Rozhodné právo 63
9.15 Shoda s právními předpisy....63
9.16 Další ustanovení....63
9.17 Další opatření 64

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

1 ÚVOD

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

1.1 Přehled

Česká pošta, s.p. (dále i Česká pošta či ČP) provozuje certifikační autoritu s názvem PostSignum VCA, která má následující hierarchii.

Název root CA: PostSignum Root QCA 4	SHA-256 otisk: AC7F7862E685C7A7D9826A58EA32D183D4 893FCC8F8FD6D900C9769A987E77F0	Platnost: 26. 7. 2038
Název podřízené CA: PostSignum Public CA 5	SHA-256 otisk: 78C0BAD095E13547B7E5646D38453393818B 2972D09B2144311B65D7EBB8B9CA	Platnost: 3. 10. 2033

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

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

Komerční certifikáty veřejného klíče vydané podle této certifikační politiky jsou určeny pro 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 nazývány žadateli o certifikát. Držitelem certifikátu je zákazník České pošty.

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

Certifikáty vydané podle této certifikační politiky mohou být použity k autentizaci, ověření serveru a ověření klienta.

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

1.2 Název a jednoznačné určení dokumentu

Certifikační autorita PostSignum potvrzuje, že tato certifikační politika je v souladu s aktuální verzí dokumentu Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [CA/B] publikovaného na http://www.cabforum.org. Pokud dojde k rozporu mezi touto certifikační politikou a [CA/B], platí ustanovení [CA/B].

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

Tab. 1 Identifikace politiky

Název dokumentu	Certifikační politika PostSignum Public CA pro komerční doménové certifikáty
Verze dokumentu	5.1.0
Stav	finální
OID poskytovatele certifikačních služeb	2.23.134
OID PostSignum Root QCA	2.23.134.1.4.2.1
OID PostSignum Public CA	2.23.134.1.2.2.3
OID této politiky	2.23.134.1.2.1.9.510
Datum vydání	10.2.2026
Datum účinnosti	10.3.2026
Datum revize	
Doba platnosti	Do odvolání nebo do dne ukončení služeb autorit PostSignum VCA.

1.2.1 Revize dokumentu

Revize dokumentu je prováděna minimálně jedenkrát za rok.

Verze	Datum revize	Důvod a popis změny	Autor	Schválil
1.0	1. 4. 2012	První verze – interní certifikační politika	PCA ČP	PAA ČP
2.0	10. 1. 2014	Certifikační politika pro veřejnost	PCA ČP	PAA ČP
3.0	4. 5. 2017	Změna vydávající autority, změna profilu certifikátu	PCA ČP	PAA ČP
4.0	8. 7. 2019	Změny v souvislosti s novou kořenovou CA, změna profilu certifikátu (CT logy)	PCA ČP	PAA ČP
4.0.1	3. 12. 2020	Revize dokumentu bez změny	PCA ČP	
4.0.2	30.11.2021	Revize dokumentu bez změny	PCA ČP	
5.0.0	3. 8. 2022	Změny v souladu s BR CA/B	PCA ČP	PAA ČP
5.0.1	15. 10. 2022	Změna profilu certifikátu – odstraněny OU	PCA ČP	PAA ČP
5.0.2	15. 8. 2023	Revize dokumentu - přidání popisu důvodů zneplatnění	PCA ČP	PAA ČP
5.0.3	15. 8. 2024	Revize dokumentu bez změny	PCA ČP	
5.0.4	15. 8. 2025	Revize dokumentu bez změny	PCA ČP	
5.1.0	9.2.2026	Změny v souladu s CCADB/ Mozilla.	PCA ČP	PAA ČP

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

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

1.3.1 Certifikační autority (dále „CA“)

Úkolem CA PostSignum VCA je především vydávat a spravovat certifikáty PostSignum Public CA a zákazníků České pošty v souladu s definovanými certifikačními politikami.

Podrobné informace o CA jsou uvedeny na webových stránkách poskytovatele www.postsignum.cz.

1.3.2 Registrační autority (dále „RA“)

Služby registračních autorit jsou zajišťovány pouze poskytovatelem certifikačních služeb. Externí subjekty nemohou poskytovat žádné služby v souvislosti s vydáním certifikátu dle této certifikační politiky.

Registrační autority zajišťují zejména tyto služby:

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

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

1.3.3 Držitelé komerčních certifikátů, kteří požádali o vydání komerčního 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 VCA. Spoléhající se strany nevstupují do smluvního vztahu s poskytovatelem certifikačních služeb.

1.3.5 Jiné participující subjekty

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

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

Komerční certifikáty vydané podle této certifikační politiky mohou být použity k autentizaci, ověření serveru a ověření klienta.

1.4.2 Omezení použití certifikátu

Komerční 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.

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

1.5 Správa politiky

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

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.

Hlášení o možné kompromitaci soukromého klíče nebo další případné zneužití certifikátu nebo jiné typy podvodu je možné taktéž hlásit na výše uvedenou e-mailovou adresu.

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

CAA – CAA záznam udává oprávnění k vydání SSL certifikátu konkrétní certifikační autoritou.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

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 – kvalifikovaný certifikát ve smyslu [eIDAS].

Kvalifikované elektronické časové razítko – kvalifikované elektronické časové razítko ve smyslu [eIDAS], v textu může být nazváno také jako kvalifikované časové razítko nebo jen časové razítko.

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

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

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

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

Ověřovací registrační autorita – zajišťuje vybrané služby registrační autority.

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

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.

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.

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

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES včetně navazujících právních předpisů.

Podepisující osoba – osoba definovaná [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 samopodepsaný 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.

QCA ČP – viz PostSignum QCA.

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

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

Secure bug Bugzilla – systém pro hlášení incidentů v souvislosti s vydáváním SSL certifikátů.

Závažná zranitelnost - Mezi závažné zranitelnosti patří kritická zranitelnost softwaru a webových aplikací, chybná API, která by mohla vést k narušení bezpečnosti dat, zero-day útoky a malware infekce.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

Bezpečnostní incident - Mezi bezpečnostní incidenty patří:

- Úspěšně provedené neoprávněné přístupy, získání, zveřejnění nebo krádeže citlivých dat, nebo zařízení CA zahrnující systémy, infrastrukturu, sítě, aplikace nebo citlivé informace CA (soukromé klíče, uživatelské přihlašovací údaje, nebo osobně identifikovatelné údaje).
- Útoky ransomwaru nebo jiné problémy s integritou dat, které nenávratně poškozují, nebo ohrožují citlivá data CA.
- Potvrzené pokročilé přetrvávající hrozby, které se pokoušejí ohrožovat infrastrukturu, systémy CA, nebo spolehlivost či platnost certifikátů.

Pokud dojde k rozporu mezi touto certifikační politikou a ustanovením odkazované sekce "How_to_Disclose_a_Reportable_Vulnerability", pak platí odkázané ustanovení v této sekci: https://wiki.mozilla.org/CA/Vulnerability_Disclosure#How_to_Disclose_a_Reportable_Vulnerability

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.

TXT DNS záznam – využívá se pro ověření vlastnictví domény při vydání SSL certifikátu jako jedna z ověřovacích metod.

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

VCA ČP – viz PostSignum VCA.

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

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

Zákazník – 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 a označující fyzickou osobu.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

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.

Tento dokument je dostupný na webových stránkách poskytovatele:

https://www.postsignum.cz/certifikacni_politiky_vca.html

2.2 Zveřejňování informací a dokumentace

Vydané certifikáty jsou uloženy v databázi certifikační autority.

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

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

Certifikační autorita PostSignum potvrzuje, že tato certifikační politika je v souladu s aktuální verzí dokumentu Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [CA/B] publikovaného na http://www.cabforum.org. Pokud dojde k rozporu mezi touto certifikační politikou a [CA/B], platí ustanovení [CA/B].

2.2.1 Zveřejňování certifikátů a CRL

Certifikáty certifikačních autorit jsou zveřejňovány

- na webových stránkách poskytovatele

  www.postsignum.cz, nebo

  www.postsignum.eu.

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, certifikační prováděcí směrnice, zpráva pro uživatele, auditní zprávy a případně i další dokumenty jsou zveřejňovány na

- webových stránkách poskytovatele.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

Další důležité informace (např. zneplatnění certifikátu 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.

2.2.3 Testovací webové stránky

Na těchto webových stránkách jsou k dispozici níže uvedené stavy doménového certifikátu k otestování:

- platný: https://www.postsignum.eu:8443/
- prošlý: https://www.postsignum.eu:8444/
- zneplatněný: https://www.postsignum.eu:8445/

2.3 Periodicita zveřejňování informací

Informace jsou zveřejňovány v následujících intervalech:

- certifikační politiky, certifikační prováděcí směrnice a zpráva pro uživatele jsou revidovány minimálně jedenkrát za rok a zveřejňovány po schválení a vydání nové verze. Verzování dokumentu se řídí dle kapitoly 9.12.3.
- 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 jsou zveřejňovány neprodleně.

2.4 Řízení přístupu a úložiště

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.

Precertifikáty i certifikáty jsou vždy zveřejněny v příslušném CT logu. Žadatel si může zvolit, zda bude certifikát zveřejněn na webových stránkách poskytovatele.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

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.

Musí být v souladu s [CA/B] a RFC5280.

Jméno certifikátu (CN) ani položka Subject Alternative Name nesmí obsahovat IP adresu nebo název lokální domény (např. .local).

Doménové názvy IDN nejsou povoleny.

3.1.2 Požadavek na významovost jmen

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

3.1.3 Anonymita a používání pseudonymu

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

3.1.4 Pravidla pro interpretaci různých forem jmen

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

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

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

3.1.5 Jedinečnost jmen

Každý zákazník v systému certifikační autority má přiřazen jedinečný identifikátor, který je uložen v údaji „serialNumber“ v Subjectu certifikátu.

V položce Subject certifikátu je uvedena kombinace jednoznačných údajů o zákazníkovi (IČO zákazníka a jméno zákazníka) a jednoznačného rozlišovacího jména.

3.1.6 Obchodní značky

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

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

3.2 Počáteční ověření identity

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

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

3.2.2 Ověřování identity právnické osoby nebo organizační složky státu

Následující ustanovení jsou platná rovněž pro 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.

3.2.2.1 Ověřování identity zákazníka

Totožnost zákazníka je ověřována na základě IČO z důvěryhodných veřejných rejstříků, jako je obchodní rejstřík nebo živnostenský rejstřík, provozovaných orgánem veřejné moci v jehož jurisdikci je vznik, či uznání Subjektu (dále též jako „Spolehlivý zdroj dat“).

3.2.2.2 Ověřování obchodního jména

Obchodní jméno zákazníka je ověřováno ze Spolehlivého zdroje dat..

3.2.2.3 Ověřování země sídla zákazníka

Země sídla zákazníka je ověřováno ze Spolehlivého zdroje dat.

3.2.2.4 Ověřování doménového jména zákazníka (FQDN)

Ověření FQDN je prováděno v souladu s [CA/B] kapitolami 3.2.2.4.4 (zaslání ověřovacího e-mailu na konstruovaný e-mail v požadované doméně) a 3.2.2.4.7 (ověření DNS TXT záznamu) obsahující náhodnou hodnotu s platností 30 dní. Náhodná hodnota je vytvářena pomocí generátoru náhodných hodnot s hashem SHA256.

Ostatní metody ověření doménového jména nejsou povolené.

Ověření vlastnictví domény se provádí odesláním ověřovacího e-mailu na jednu z pevných e-mailových adres vybraných během registrace. E-mailová adresa je vždy z domény, jejíž název má být vložen do názvu certifikátu nebo do přípony certifikátu.

V případě ověření pomocí DNS TXT záznamu je zákazníkovi předán během registračního procesu řetězec, který je nutné do DNS TXT záznamu vložit. Tento řetězec je před vydáním certifikátu ověřen.

Způsob ověření FQDN je archivován.

RA nikdy nedeleguje ověřování FQDN na jiný subjekt.

Všechna data v certifikátu před vydáním, a to jak data domény, tak i data subjektu jsou ověeny ze Spolehlivého zdroje dat.

3.2.2.5 Ověřování IP adresy

Vloženo IP adresy do certifikátu není povoleno.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

3.2.2.6 Ověřování wildcard domény

Domény se zástupnými znaky (wildcard) jsou povoleny na druhé a vyšší úrovni. Ověření se provádí v souladu s kapitolou 3.2.2.4. Certifikáty se zástupnými znaky podléhají zvláštní kontrole pro domény jiné než .cz. CA před vydáním kontroluje seznam veřejných přípon na adrese https://publicsuffix.org/.

3.2.2.7 Přesnost zdroje dat

Pro ověřování dat vkládaných do certifikátu se využívají pouze Spolehlivý zdroj dat. Česká pošta stanovila, že tyto zdroje jsou spolehlivými zdroji dat v souladu s [CA/B].

3.2.2.8 CAA záznamy

Během procesu registrace je před vydáním certifikátu ověřen záznam CAA domény pro každý dNSName v příponě subjectAltName. Při zpracování záznamů CAA CA zpracovává issuewild dle specifikace v RFC 8659.

Pokud je záznam CAA pro požadovanou doménu neúplný nebo obsahuje název domény postsignum.cz, je žádost o vydání certifikátu akceptována. Pokud záznam CCA pro požadovanou doménu obsahuje jiný název domény než postsignum.cz, je žádost o vydání certifikátu zamítnuta.

Záznam CAA je ověřen po 8 hodinách od přijetí žádosti o vydání certifikátu CA.

Příznak kritický má výchozí hodnotu 0, v případě nesrovnalosti probíhá ruční zpracování. V případě jakýchkoli problémů CA kontaktuje žadatele o certifikát domény. CA nepodporuje záznam iodef a výjimky nejsou uvedeny v CP.

V případě podezření na zneužití certifikátu domény neoprávněnou osobou bude tato skutečnost nahlášena [CA/B]..

3.2.3 Ověřování identity fyzické osoby

3.2.3.1 Ověření identity žadatele o vydání certifikátu

Identita žadatele se ověřuje pomocí e-mailové adresy během procesu vydání certifikátu, viz kapitola 4.2.

3.2.3.2 Ověření identity žadatele v případě zneplatnění certifikátu

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

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 a nevykazuje známky pozměnění nebo padělání. Totožnost osoby se ověřuje pouze v případě zneplatnění a předložený dokument se kontroluje, zda nebyl pozměněn nebo padělán.

- Občané České republiky musí předložit originál občanského průkazu nebo cestovního pasu.

- Cizinci musí předložit originál cestovního, diplomatického, služebního nebo jinak nazývaného pasu vydaného cizím státem nebo samostatného průkazu o povolení k pobytu vydávaný orgány ČR.
  Občané členských států Evropské unie a dále občané Islandu, Lichtenštejnska, Norska a Švýcarska mohou předložit také originál osobního dokladu, který jim byl vydán k prokazování totožnosti na území příslušného státu.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

3.2.4 Neověřené informace vztahující se k držiteli certifikátu

Vydaný certifikát obsahuje pouze ověřené informace certifikační autoritou.

3.2.5 Ověřování specifických práv

Česká pošta, jakožto poskytovatel certifikačních služeb ověřuje oprávnění žádat o certifikát dle této certifikační politiky. Oprávnění žádat o certifikát přiděluje pověřená osoba zákazníka.

Vytvoření žádosti o certifikát je možné pouze prostřednictvím Zákaznického portálu poskytovatele.

3.2.6 Kritéria pro interoperabilitu

Spolupráce s jinými poskytovateli certifikačních služeb není možná.

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

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

V případě žádosti o vydání následného certifikátu je nutné při identifikaci a autentizaci spojené s vydáním nového certifikátu postupovat jako v případě počátečního ověření identity při vydání prvního certifikátu (viz kapitola 4.2).

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 4.2).

3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu

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

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

Pověřená osoba prokáže svou totožnost:

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

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

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

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.

Žádosti o vydání certifikátů jsou zpracovávány přímo pracovníky registrační autority. Je tak zajištěno, že podezřelé žádosti o vydání certifikátu jsou zachyceny a zamítnuty.

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 může být uzavřena v písemné nebo elektronické formě.

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

4.1.2.2 Pre-registrace žadatelů o certifikát

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

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.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

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

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

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.

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.

4.1.2.5 Odpovědnost žadatele

Žadatel je povinen zejména:

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

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

- po vygenerování párových dat (soukromý a veřejný klíč) provést neprodleně jejich zálohu.

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, vydat rozhodnutí, zda bude certifikát vydán, a o tomto rozhodnutí informovat žadatele nebo zákazníka,
- vydat certifikát obsahující věcně správné údaje na základě informací, které jsou certifikační autoritě k dispozici v době vydávání certifikátu,
- zveřejňovat certifikační politiky, podle kterých vydává certifikáty, na webových stránkách poskytovatele, případně jinými vhodnými způsoby (viz. kapitola 2.2),
- zveřejnit kvalifikovaný 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

Identita žadatele je ověřena na základě e-mailové adresy zadané pověřenou osobou. V případě, že identita žadatele není ověřena, není povoleno tomuto žadateli požádat o certifikát.

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 elektronicky způsobem upřesněným na webových stránkách poskytovatele. PKCS#10 žádost nemůže být po vydání certifikátu znovu použita.

Do certifikátu budou vloženy údaje dle platného seznamu žadatelů předané pověřenou osobou.

Dále jsou před vydáním certifikátu prováděny následující kontroly:

FQDN: Pokud údaje o vydání certifikátu obsahují neúplné nebo nepovolené FQDN (IP adresa, lokální doména), je taková žádost zamítnuta. V certifikátu musí být uvedeno minimálně jedno FQDN, které je zároveň uvedeno i v SAN.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

Ověření FQDN dle kapitoly 3.2.2.4 vede ke schválení nebo zamítnutí žádosti.

Ověřená data nelze využít pro vydání jiného certifikátu se stejným doménovým názvem, kontrola FQDN a ověření žádosti o vydání certifikátu je prováděno před každým vydáním certifikátu.

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

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

V případě zamítnutí žádosti je tato žádost archivována z důvodu podezření na podvodné jednání.

4.2.2.2 Přijetí nebo zamítnutí žádosti o následný certifikát

Následný certifikát dle této certifikační politiky není povolené vydávat. Při žádosti o certifikát se postupuje dle kapitoly 4.2.2.1

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 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

Pracovníci registrační autority provedou kontrolu žádosti dle kapitoly 4.2.2.1 a předají žádost certifikační autoritě.

Certifikační autorita vystaví pre-certifikát, který publikuje do CT logů v souladu s RFC 6962. Precertifikát je zasílán minimálně do 3 CT logů. Seznam CT logů, do kterých jsou pre-certifikáty zasílány, je uveden na webových stránkách poskytovatele.

V případě zneplatnění certifikátu je vždy automaticky zneplatněn i precertifikát. Certifikát je vydán systémem certifikační autority automaticky po obdržení ID záznamu z CT logů.

4.3.2 Oznámení o vydání certifikátu držiteli certifikátu

Na e-mailovou adresu žadatele je odeslána informace o umístění vydaného certifikátu (URL), kde je možné vydaný certifikát 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.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

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 žadateli předán ve formátu DER, PEM.

4.4.2 Zveřejňování vydaných certifikátů poskytovatelem

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

4.4.3 Oznámení o vydání certifikátu jiným subjektům

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

4.5 Použití párových dat a certifikátu

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

4.5.1 Použití soukromého klíče a certifikátu držitelem certifikátu

Držitel certifikátu:

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

4.5.2 Použití veřejného klíče a certifikátu spoléhající se stranou

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

- získá certifikáty PostSignum Public CA a PostSignum Root QCA z bezpečného zdroje (webové stránky poskytovatele, na obchodním místě) a ověří otisk ("fingerprint") těchto certifikátů.
- před použitím certifikátu vydaného PostSignum Public CA ověří platnost certifikátu PostSignum Public CA a následně i platnost vydaného koncového certifikátu; kontrola se provádí na správnost podpisu

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

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 VCA tuto službu neposkytuje.

4.6.1 Podmínky pro obnovení certifikátu

PostSignum VCA tuto službu neposkytuje.

4.6.2 Subjekty oprávněné požadovat obnovení certifikátu

PostSignum VCA tuto službu neposkytuje.

4.6.3 Zpracování požadavku na obnovení certifikátu

PostSignum VCA tuto službu neposkytuje.

4.6.4 Oznámení o vydání obnoveného certifikátu držiteli certifikátu

PostSignum VCA tuto službu neposkytuje.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu

PostSignum VCA tuto službu neposkytuje.

4.6.6 Zveřejňování vydaných obnovených certifikátů poskytovatelem

PostSignum VCA tuto službu neposkytuje.

4.6.7 Oznámení o vydání obnoveného certifikátu jiným subjektům

PostSignum VCA tuto službu neposkytuje.

4.7 Výměna veřejného klíče v certifikátu

PostSignum VCA tuto službu neposkytuje.

4.8 Změna údajů v certifikátu

Certifikát se změněnými údaji lze vydat pouze

- jako nový certifikát podle postupů uvedených v kapitolách 4.1 - 0, nebo

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

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

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

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).

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

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

Telefon: 954 303 303

- e-mailem (nonstop)

E-mail: postsignum@cpost.cz

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

- 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

4.9.1.1 Důvody pro zneplatnění certifikátu koncového uživatele

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

Certifikační autorita PostSignum umožňuje zvolit jeden z následujících důvodů zneplatnění:

- unspecified - nespecifikováno 0 Znamená, že nelze použít žádný z níže uvedených důvodů. V tomto případě není v CRL uveden důvod zneplatnění.

- keyCompromise – kompromitace klíče 1 - Znamená, že je známo nebo existuje podezření, že soukromý klíč žadatele byl ohrožen. CA Postsignum neočekává, že obdrží důkazy o ohrožení klíče.

- affiliationChanged – změna vlastníka 3 - Znamená, že se jméno subjektu nebo jiné informace o identitě subjektu v certifikátu změnily, ale neexistuje důvod k podezření, že soukromý klíč certifikátu byl ohrožen.

- superseded – nahrazení certifikátu 4 - Znamená, že certifikát je nahrazován, protože: žadatel požádal o nový certifikát, CA má rozumné důkazy o tom, že by se nemělo spoléhat na ověření autorizace domény nebo kontroly pro jakýkoli plně kvalifikovaný název domény, nebo CA zrušila certifikát z důvodů souladu, například proto, že certifikát nesplňuje tyto základní požadavky CP nebo CPS.

- cessationOfOperation – skončení operace 5 – Znamená, že zabezpečená webová stránka certifikátem již není aktivní před vypršením platnosti certifikátu, nebo pokud žadatel již certifikát před vypršením jeho platnosti nevlastní ani neovládá.

- privilegiumWithdrawn – odejmuto oprávnění 9 – Znamená, že došlo k porušení na straně žadatele, které nevedlo k ohrožení klíče, například žadatel certifikátu poskytl zavádějící informace ve své žádosti o certifikát nebo nedodržel své podstatné povinnosti vyplývající ze smlouvy s žadatelem nebo této certifikační politiky. Tento důvod zneplatnění může použít pouze certifikační autorita při zneplatnění z její vůle.

V případě události lze zaslat upozornění na e-mail incident.postsignum@cpost.cz

Certifikát je ve všech případech zneplatněn do 24 hodin od přijetí žádosti ke zneplatnění.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

4.9.1.2 Důvody pro zneplatnění certifikátu podřízené certifikační autority

Viz kapitola 5.7.3.1.

4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

O zneplatnění certifikátu může požádat:

- zákazník (držitel certifikátu) prostřednictvím pověřené osoby nebo statutárního zástupce,
- žadatel o certifikát,
- Manažer CA.

4.9.3 Požadavek na zneplatnění certifikátu

4.9.3.1 Žádost o zneplatnění certifikátu podaná osobně žadatelem na registrační autoritě

Žadatel požádá o zneplatnění certifikátu osobně na pracovišti registrační autority, kde prokáže svou totožnost (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 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 e-mailovou adresu uvedenou ve zneplatněném certifikátu (pokud certifikát adresu elektronické pošty obsahuje) a na kontaktní e-mailovou adresu žadatele uvedenou v systému certifikační autority.

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.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

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

4.9.3.4 Zneplatnění certifikátu z vůle certifikační autority

O zneplatnění certifikátu může rozhodnout rovněž poskytovatel certifikačních služeb, pokud žadatel o certifikát nebo zákazník porušují pravidla certifikační politiky nebo dohodnuté smluvní podmínky. PostSignum VCA v takovém případě informuje zákazníka o zneplatnění certifikátu s udáním důvodu, proč byl certifikát 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 adresu uvedenou ve zneplatněném certifikátu (pokud certifikát adresu elektronické pošty obsahuje) a na kontaktní adresu žadatele uvedenou v systému certifikační autority.

4.9.3.5 Hlášení problému s certifikátem

Žadatelé, spoléhající se strany, dodavatelé aplikačního softwaru a další třetí strany mohou hlásit podezření na kompromitaci soukromého klíče, zneužití certifikátu nebo jiné typy podvodu, kompromitaci, zneužití, nevhodné chování nebo jakoukoli jinou záležitost související s certifikáty. Možné kompromitace soukromého klíče nebo jiné možné zneužití certifikátu či jiné typy podvodu lze také hlásit na e-mailovou adresu: incident.postsignum@cpost.cz

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 Public CA (spoléhající se strana) je povinen postupovat v souladu s ustanoveními kapitoly 4.5.1.

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. Seznam zneplatněných certifikátů je zveřejňován na těchto místech:

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

Frekvence vydávání CRL pro podřízené certifikační autority je jednou za 12 měsíců od posledního vydání.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

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“)

Následující podmínky platí pro komunikaci stavu certifikátů, které zahrnují rozšíření přístupu k informacím o autoritě s metodou přístupu id-ad-ocsp. Odpovědi OCSP odpovídají normám RFC6960. Odpovědi OCSP jsou:
Podepsány respondérem OCSP, jehož certifikát je podepsán certifikační autoritou, která vydala certifikát, jehož stav odvolání se kontroluje.

URL adresa OCSP služby je uvedena ve vydaném certifikátu dle této certifikační politiky, viz profil certifikátu v kapitole 7.1.2

4.9.10 Požadavky při ověřování statutu certifikátu on-line

Následující podmínky platí pro komunikaci stavu certifikátů, které obsahují rozšíření Authority Information Access s metodou accessMethod id-ad-ocsp. OCSP respondéry provozované CA podporují metodu HTTP GET, jak je popsáno v RFC 6960.

CA zpracovává rozšíření Nonce (1.3.6.1.5.5.7.48.1.2) v souladu s RFC 8954. Interval platnosti odpovědi OCSP je časový rozdíl mezi polem thisUpdate včetně. Pro účely výpočtu rozdílů se rozdíl 3 600 sekund rovná jedné hodině a rozdíl 86 400 sekund se rovná jednomu dni, bez započítání přestupných sekund. Toto platí i pro podřízený certifikát.

Informace o aktualizaci CA poskytované prostřednictvím protokolu Online Certificate Status Protocol

i. alespoň každých dvanáct měsíců; a

ii. do 24 hodin po zrušení certifikátu podřízené CA. Pokud respondent OCSP obdrží požadavek na stav sériového čísla certifikátu, který je „unspecified“, pak respondent neodpoví stavem „good“.

Pro ověření certifikátu vydaného dle této certifikační politiky je možné využít veřejně dostupnou službu OCSP. OCSP služba je provozována v režimu 24/7 a poskytována dle standardu RFC 6960. Formát žádosti a odpovědi OCSP je uveden v kapitole 7.3.

4.9.11 Jiné způsoby oznamování zneplatnění certifikátu

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

4.9.12 Případné odlišnosti postupu zneplatnění v případě kompromitace soukromého klíče

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

4.9.13 Podmínky pro pozastavení platnosti certifikátu

PostSignum VCA tuto službu neposkytuje. Platnost certifikátu nelze pozastavit.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

4.9.14 Subjekty oprávněné požadovat pozastavení platnosti certifikátu

PostSignum VCA tuto službu neposkytuje.

4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu

PostSignum VCA tuto službu neposkytuje.

4.9.16 Omezení doby pozastavení platnosti certifikátu

PostSignum VCA tuto službu neposkytuje.

4.10 Služby související s ověřováním stavu certifikátu

Status certifikátu je možné ověřit

- na seznamu zneplatněných certifikátů (CRL) v rámci služby umožňující přístup k veřejným informacím PostSignum VCA protokolem HTTP, nebo
- v rámci služby vyhledávání vydaných certifikátů přístupné na webových stránkách 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. Informace o zneplatnění certifikátu je v CRL uvedena minimálně do doby jeho platnosti.

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, která musí splňovat náležitosti uvedené v certifikační prováděcí směrnici. Odpověď OCSP serveru je podepsaná certifikátem OCSP serveru a má předepsaný formát, uvedený v certifikační prováděcí směrnici. 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. Za normálních provozních podmínek je odezva na získání těchto informací 10 sekund a méně.

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

Veřejná služba OCSP je dostupná 7 dní v týdnu 24 hodin denně.

V případě nedostupnosti lze zaslat na e-mail incident.postsignum@cpost.cz

4.10.3 Další charakteristiky služeb statutu certifikátu

Další charakteristiky služeb statutu certifikátu nejsou stanoveny.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

4.11 Ukončení poskytování služeb pro držitele certifikátu

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

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

4.12 Úschova soukromého klíče u důvěryhodné třetí strany a jejich obnova

PostSignum VCA tuto službu neposkytuje.

4.12.1 Politika a postupy při úschově a obnovování soukromého klíče

PostSignum VCA tuto službu neposkytuje.

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

PostSignum VCA tuto službu neposkytuje.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

5 MANAGEMENT, PROVOZNÍ A FYZICKÁ BEZPEČNOST

Pro PostSignum VCA byly zpracovány dokumenty:

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

Výše uvedené dokumenty byly vypracovány na základě výsledků analýzy rizik. Bezpečnostní program certifikační autority zahrnuje každoroční hodnocení rizik, které:

1. Identifikuje předvídatelné vnitřní a vnější hrozby, jež by mohly vést k neoprávněnému přístupu, zveřejnění, zneužití, změně nebo zničení jakýchkoli dat certifikátu nebo procesů správy certifikátů;

2. Posuzuje pravděpodobnost a potenciální škody způsobené těmito hrozbami s přihlédnutím k citlivosti dat certifikátu a procesů správy certifikátů; a

3. Posuzuje dostatečnost politik, postupů, informačních systémů, technologií a dalších opatření, která má certifikační autorita zavedena k boji proti těmto hrozbám.

Analýza rizik se provádí a vyhodnocuje v souladu s interními předpisy České pošty.

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

5.1 Fyzická bezpečnost

5.1.1 Umístění a konstrukce

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

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

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

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

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 nainstalovánu klimatizaci, která udržuje teplotu a vlhkost optimální pro provozovaná zařízení.

5.1.4 Vlivy vody

Centrální pracoviště jsou umístěna mimo zátopové oblasti.

Prostory centrálních pracovišť jsou vybaveny signalizací zatopení vodou.

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 VCA jsou k dispozici trezory, minimálně jeden z nich je umístěn mimo areály budov centrálních pracovišť.

5.1.7 Nakládání s odpady

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

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

5.1.8 Zálohy mimo budovu

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

5.2 Procesní bezpečnost

5.2.1 Důvěryhodné role

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

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

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

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

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

5.2.3 Identifikace a autentizace pro každou roli

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

5.2.4 Role vyžadující rozdělení povinností

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

5.3 Personální bezpečnost

5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

Role, zajišťující provoz, správu, údržbu a rozvoj systémů PostSignum VCA jsou obsazovány na základě procedur (např. vyžadování referencí, zkušební období apod.), které zajišťují, aby tyto funkce byly obsazovány důvěryhodnými, kvalifikovanými a bezúhonnými 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 VCA 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 VCA, jsou vyškoleni, primárně operátoři RA vykonávající roli specialisty ověření. Operátoři RA jsou školeni jednou ročně a o absolvování školení musí být veden záznam.. 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.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

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

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

5.3.4 Požadavky a periodicita školení

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

Manažer VCA v pravidelných intervalech (zejména při změnách v postupech PostSignum VCA) 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, viz kapitola 5.3.3.

5.3.8 Dokumentace poskytovaná zaměstnancům

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

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

5.4 Auditní záznamy (logy)

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

5.4.1 Typy zaznamenávaných událostí

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

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

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

Záznamy v deníku obsahují následující prvky:

1. Datum a čas záznamu;

2. Totožnost osoby, která záznam v deníku provádí; a

3. Popis záznamu.

Žádná z těchto operací není povolena třetí straně.

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 uložené v různých lokalitách.

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

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

5.4.7 Postup při oznamování události subjektu, který ji způsobil

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

5.4.8 Hodnocení zranitelnosti

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

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

Minimálně 1x za rok jsou prováděny kontroly zranitelnosti systémů certifikační autority.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

5.5 Uchovávání informací a dokumentace

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

5.5.1 Typy informací a dokumentace, které se uchovávají

V PostSignum VCA se archivují tyto záznamy:

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

5.5.2 Doba uchování uchovávaných informací a dokumentace

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

5.5.3 Ochrana úložiště uchovávaných informací a dokumentace

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

5.5.4 Postupy při zálohování uchovávaných informací a dokumentace

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

5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

Pokud jsou v PostSignum VCA 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 VCA 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 veřejného klíče elektronických pečetí v nadřízeném certifikátu pro elektronickou pečeť poskytovatele

Platnost klíčů certifikačních autorit v hierarchii PostSignum VCA je omezena.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

S dostatečným předstihem, avšak nejméně 1 rok před vypršením platnosti certifikátu PostSignum Root QCA se musí uskutečnit ceremoniál vydání nového certifikátu. Výsledkem ceremoniálu bude vytvořený nový samopodepsaný certifikát kořenové certifikační autority, který bude zveřejněn způsobem popsaným v kapitole 0.

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

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

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

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

5.7 Obnova po havárii nebo kompromitaci

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

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

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

5.7.1 Postup v případě incidentu a kompromitace

Zabezpečení prostředků certifikační autority po živelní katastrofě nebo jiné mimořádné události je rozpracováno v dokumentech Krizový plán ochrany objektu a Plán zvládání krizových situací a plán obnovy. Testy havarijního plánu ověřuje alespoň jednou ročně externí auditor.

Certifikační autorita udržuje komplexní a proveditelný plán pro hromadné zneplatnění certifikátů a provádí každoroční testování hromadného zneplatnění.

Plán hromadného zneplatnění zahrnuje jasně definované, proveditelné a komplexní postupy určené k zajištění rychlé, konzistentní a spolehlivé reakce na rozsáhlé scénáře zneplatnění certifikátů. Plán hromadného zneplatnění je integrován do plánu obnovy po havárii.

5.7.2 Poškození výpočetních prostředků, softwaru nebo dat

V případě bezpečnostního incidentu kompromitace klíčů certifikačních autorit popsaných v kapitolách 5.7.3 jsou tyto incidenty nahlášeny do Secure bug Bugzilla.Zabezpečení prostředků certifikační autority po živelní katastrofě nebo jiné mimořádné události je rozpracováno v dokumentech Krizový plán ochrany objektu a Plán zvládání krizových situací a plán obnovy.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

5.7.3 Postup při kompromitaci dat pro vytváření elektronických pečetí poskytovatele

5.7.3.1 Kompromitace soukromého klíče podřízené certifikační autority

V případě podezření na kompromitaci soukromého klíče PostSignum Public CA budou písemně nebo elektronicky informováni všichni držitelé certifikátů 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 VCA a v jednom celostátně vydávaném deníku. Součástí oznámení bude i důvod ukončení platnosti certifikátu certifikační autority.

PostSignum Root QCA okamžitě, nejpozději do 7 dní, zneplatní certifikát PostSignum Public 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 Public CA.

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

Tento postup bude také použit v případě, kdy dojde k náhlému oslabení algoritmu použitého pro vytváření elektronických pečetí, které nepopiratelně 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, nejpozději do 7 dní, 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 VCA 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 pečetí PostSignum Root QCA, která sloužila pro podepisování kvalifikovaných certifikátů a seznamů zneplatněných certifikátů, u nichž existuje podezření na kompromitaci, a o tomto zničení provede záznam.

Tento postup bude také použit v případě, kdy dojde k náhlému oslabení algoritmu použitého pro vytváření elektronických pečetí, které nepopiratelně 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 zvládání krizových situací a plán obnovy.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

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 VCA. 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 pečetí PostSignum Root QCA, která sloužila pro pečetění kvalifikovaných certifikátů a seznamů zneplatněných certifikátů, a o tomto zničení provede záznam. Záznamy budou uchovávány v souladu s ustanoveními této certifikační politiky uvedenými v kapitole **Chyba! Nenalezen zdroj odkazů.**.

5.8.2 Ukončení činnosti podřízené certifikační autority

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

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

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

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

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

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

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.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

6 TECHNICKÁ BEZPEČNOST

6.1 Generování a instalace párových dat

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

6.1.1 Generování párových dat

Klíčové páry certifikačních autorit v hierarchii PostSignum VCA 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, jako je systém RA, nebo systémů PostSignum VCA (infrastrukturní klíče) jsou generovány v kontrolovaném prostředí systémů PostSignum VCA. Tyto klíčové páry jsou uloženy v kryptografickém modulu; pro přístup k těmto klíčovým párům je nutné vložit čipovou kartu obsluhy a 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 VCA nepředepisuje konkrétní požadavky na příslušné úložiště (není předepsáno používání prostředku pro bezpečné vytváření elektronických podpisů). PostSignum VCA negeneruje soukromé klíče žadatelům.

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

Kontrola kvality veřejných klíčů se provádí v souladu s odstavcem 6.1.6.

6.1.2 Předání soukromého klíče žadateli o certifikát

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

6.1.3 Předání veřejného klíče poskytovateli certifikačních služeb

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

6.1.4 Poskytování veřejného klíče certifikační autoritou spoléhajícím se stranám

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

6.1.5 Délky párových dat

Klíče certifikačních autorit v hierarchii PostSignum mají pro algoritmus RSA délku modulu 4096 bitů.

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

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

6.1.6 Generování parametrů veřejného klíče a kontrola jejich kvality

Parametry používané při vytváření veřejných klíčů komponent PostSignum VCA jsou generovány odpovídajícím softwarovým a hardwarovým vybavením. Použité algoritmy a jejich parametry odpovídají požadavkům technických norem.

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

Kontrola kvality veřejných klíčů je nastavena na úrovni certifikační autority, která kontroluje jedinečnost a povolenou délku veřejného klíče. V případě, že je k vygenerování soukromého veřejného klíče použit algoritmus, který byl narušen, si certifikační autorita vyhrazuje právo žádost odmítnout.

CA si vyhrazuje právo odmítnout žádost o certifikát, pokud nesplňuje následující požadavky:

- musí být použit odpovídající algoritmus

- odpovídající velikost klíče

- nikoliv kompromitovaný algoritmus

- unikátní klíč (nepoužitý)

6.1.7 Omezení pro použití klíče

Klíče koncových uživatelů mohou být použity pouze v souladu s pravidly popsanými v kapitole 1.4.

Klíče certifikační autority PostSignum Root nesmí být použity pro vydání certifikátů koncových uživatelů.

6.2 Ochrana soukromého klíče a bezpečnost kryptografických modulů

CA implementuje fyzická a logická ochranná opatření, aby zabránila neoprávněnému vydávání certifikátů.

6.2.1 Standardy a podmínky používání kryptografických modulů

Během provozu je soukromý klíč certifikační autority uložen v nešifrované podobě v aktivovaném a nakonfigurovaném kryptografickém modulu (zabezpečený kryptografický modul), který může být zapnut a vypnut pouze jednou osobou.

Kryptografický modul použitý pro generování a úschovu soukromého klíče certifikačních autorit (nástroj pro vytváření elektronického podpisu) působících v hierarchii PostSignum VCA splňuje požadavky standardu FIPS 140-2 Level 3.

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.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

6.2.3 Úschova soukromého klíče

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

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

Soukromé klíče certifikačních autorit v hierarchii PostSignum VCA 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 pečetí 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 se záloh po autentizaci dvou pracovníků, kteří nemají přístup k záloze soukromého klíče a kteří nemají právo na aktivaci soukromého klíče (spuštění procesu certifikační autority).

6.2.7 Uložení dat pro vytváření elektronických pečetí 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 pečetí

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 pečetí

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 pečetí

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,

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

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 veřejných klíčů

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 a párových dat

Doba platnosti certifikátu vydaného podle této certifikační politiky je uvedena v certifikátu. Platnost certifikátu nesmí být delší než 397 dní.

6.4 Aktivační data

V systému PostSignum VCA jsou používána aktivační data různého charakteru, například přístupová hesla, PIN a jiné. Všechny aspekty týkající se aktivačních dat, jejich generování, instalace a používání, jsou popsány v interních dokumentech Systémová 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 prozrazením neoprávněné osobě. Příslušné povinnosti v tomto smyslu mají všichni pracovníci PostSignum VCA a jsou uvedeny v interním dokumentu Systémová bezpečnostní politika.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

6.4.3 Ostatní aspekty aktivačních dat

Ostatní aspekty týkající se aktivačních dat, jejich generování, instalace a používání, jsou popsány v interních dokumentech Systémová 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 VCA jsou definována nastavení zajišťující bezpečnost dané komponenty na technologické úrovni, která vycházejí ze standardů [ETSI EN 319 401], [ETSI EN 319 411] a [CA/B].

Všichni operátoři RA, kteří vydávají certifikáty koncovým uživatelům mají do systému RA přístup zajištěný vícefaktorovou autentizací, viz kapitola 6.1.1.4.

6.5.2 Hodnocení počítačové bezpečnosti

Systém PostSignum VCA prošel po vybudování externí kontrolou bezpečnostní shody zaměřenou na splnění požadavků uvedených v [CA/B].

6.6 Bezpečnost životního cyklu

6.6.1 Řízení vývoje systému

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

Následné změny jsou realizovány v souladu s definovaným změnovým řízením.

6.6.2 Kontroly řízení bezpečnosti

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

6.6.3 Řízení bezpečnosti životního cyklu

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

6.7 Síťová bezpečnost

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

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

Veškerá komunikace mimo vyhrazené lokální sítě centrálních pracovišť je šifrovaná.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

Kontrola síťové bezpečnosti je prováděna kontinuálně pomocí nástrojů na vyhodnocení bezpečnostních hrozeb. Jedenkrát za rok je prováděna kontrola na zabezpečení sítě.

V případě narušení bezpečnosti sítě je okamžitě zastaven provoz všech komponent certifikační autority.

Síťová bezpečnost systémů certifikační autority je v souladu s NCSSR.

6.8 Časová razítka

Viz kapitola 5.5.5.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

7 PROFILY CERTIFIKÁTU, SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ A OCSP

7.1 Profil certifikátu

PostSignum VCA vydává certifikáty odpovídající standardu X.509. Sériová čísla certifikátů jsou generována sekvenčně. Profily certifikátů kořenové, podřízené autority a profil certifikátu žadatele jsou uvedeny v následujících podkapitolách. Profil komerčního doménového certifikátu.

7.1.1 Číslo verze

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

7.1.2 Obsah a rozšiřující položky v certifikátu

Položky v certifikátu odpovídají RFC 5280.

7.1.2.1 Certifikát kořenové CA

Název položky	Hodnota/příznak použití
Version	3 (0x2)
Serial Number	*0f.a0*
SignatureAlgorithm	Sha512WithRSAEncryption
Issuer	
C countryName	CZ
organizationIdentifier	NTRCZ-47114983
O organisationName	Česká pošta, s.p.
CN commonName	PostSignum Root QCA 4
Validity	
Not Before	*26. 7. 2018 09:56:08 GMT*
Not After	*26. 7. 2038 09:56:08 GMT*
Subject	
C countryName	CZ
organizationIdentifier	NTRCZ-47114983
O organisationName	Česká pošta, s.p.
CN commonName	PostSignum Root QCA 4
Subject Public Key Info	
Algorithm	rsaEncryption
SubjectPublicKey	*Veřejný klíč*
Extensions	*rozšíření certifikátu viz tabulka níže*
Signature	*elektronická pečeť poskytovatele certifikačních služeb*

Rozšíření v certifikátu:

Název rozšiřující položky	Hodnota/příznak použití	Kritická ano/ne
Authority Key Identifier		ne
Key Identifier	*používá se*	
Subject Key Identifier	*používá se*	ne

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

Key Usage		ano
DigitalSignature	Ne	
NonRepudiation	Ne	
KeyEncipherment	Ne	
DataEncipherment	Ne	
KeyAgreement	Ne	
KeyCertSign	Ano	
CRLSign	Ano	
CertificatePolicies		ne
Policy Identifier	2.5.29.32.0 (Any Policy)	
User Notice	Tento certifikat pro elektronickou pecet byl vydan v souladu s narizenim EU c. 910/2014.This is a certificate for electronic seal according to Regulation (EU) No 910/2014.	
CRL Distribution Points		ne
URI	http://crl.postsignum.cz/crl/psrootqca4.crl	
URI	http://crl2.postsignum.cz/crl/psrootqca4.crl	
URI	http://crl.postsignum.eu/crl/psrootqca4.crl	
Basic Constraints		ano
cA	TRUE	
PathLenConstraint	1	

7.1.2.2 Certifikát podřízené CA

Název položky	Hodnota/příznak použití
Version	3 (0x2)
Serial Number	*10:6c*
SignatureAlgorithm	Sha512WithRSAEncryption
Issuer	
C countryName	CZ
organizationIdentifier	NTRCZ-47114983
O organisationName	Česká pošta, s.p.
CN commonName	PostSignum Root QCA 4
Validity	
Not Before	*3. 10. 2018 06:48:01 GMT*
Not After	*3. 10. 2033 06:48:01 GMT*
Subject	
C countryName	CZ
organizationIdentifier	NTRCZ-47114983
O organisationName	Česká pošta, s.p.
CN commonName	PostSignum Public CA 5
Subject Public Key Info	
Algorithm	rsaEncryption
SubjectPublicKey	*Veřejný klíč*
Extensions	*rozšíření certifikátu viz tabulka níže*
Signature	*elektronická pečeť poskytovatele certifikačních služeb*

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

Rozšíření v certifikátu:

Název rozšiřující položky	Hodnota/příznak použití	Kritická ano/ne
Authority Key Identifier		ne
Key Identifier	*používá se*	
Subject Key Identifier	*používá se*	ne
Key Usage		ano
DigitalSignature	Ne	
NonRepudiation	Ne	
KeyEncipherment	Ne	
DataEncipherment	Ne	
KeyAgreement	Ne	
KeyCertSign	Ano	
CRLSign	Ano	
CertificatePolicies		ne
Policy Identifier	2.5.29.32.0 (Any Policy)	
User Notice	Tento certifikat pro elektronickou pecet byl vydan v souladu s narizenim EU c. 910/2014.	
CRL Distribution Points		ne
URI	http://crl.postsignum.cz/crl/psrootqca4.crl	
URI	http://crl2.postsignum.cz/crl/psrootqca4.crl	
URI	http://crl.postsignum.eu/crl/psrootqca4.crl	
Basic Constraints		ano
cA	TRUE	
PathLenConstraint	0	
AuthorityInfoAccess		
accessMethod	id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	
URI	http://crt.postsignum.cz/crt/psrootqca4.crt	
accessMethod	id-ad-caIssuers (1.3.6.1.5.5.7.48.1)	
URI	http://ocsp.postsignum.cz/OCSP/RQCA4/	

7.1.2.3 Certifikát žadatele

Položka	**Hodnota**	**Poznámka**
Version	3 (0x2)	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.
Serial number	sériové číslo certifikátu přidělené certifikační autoritou	
SignatureAlgorithm	sha384WithRSAEncryption	
Issuer		
C countryName	CZ	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.
OID 2.5.4.97 organizationIdentifier	NTRCZ-47114983	
O organisationName	Česká pošta, s.p.	
CN commonName	PostSignum Public CA 5	
Validity		
Not Before	Počátek platnosti vydaného certifikátu (UTCTime)	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.
Not After	Konec platnosti vydaného certifikátu (UTCTime)	
Subject		

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

C countryName	kód státu z adresy sídla zákazníka	**povinné**	Údaj je doplněný na základě údajů ve veřejných rejstřících
ST stateOrProvinceName	název státu z adresy sídla zákazníka	nepovinné	Údaj je doplněný na základě údajů ve veřejných rejstřících
L localityName	název obce z adresy sídla zákazníka	**povinné**	Údaj je doplněný na základě údajů ve veřejných rejstřících.
OID 2.5.4.97 organizationIdentifier	obsahuje IČO organizace dle mezinárodních standardů ve tvaru: NTRxx-*IČO organizace*	**povinné**	Údaj je doplněný na základě údajů ve veřejných rejstřících xx je kód státu, odpovídá položce C (countryName)
O organisationName	jméno právnické osoby nebo podnikající fyzické osoby	**povinné**	Údaj je doplněný na základě údajů ve veřejných rejstřících
CN commonName	název domény (FQDN)	**povinné**	
serialNumber	jednoznačný identifikátor zákazníka přidělovaný poskytovatelem certifikačních služeb ve tvaru: D*číslo*	**povinné**	
Subject Public Key Info			
Algorithm	rsaEncryption	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.	
SubjectPublicKey	veřejný klíč o min. velikosti 2048 bitů		
Extensions	rozšíření certifikátu podle tabulky níže		
Signature	elektronická pečeť poskytovatele certifikačních služeb		

Rozšíření v certifikátu

Položka	**Hodnota**	**Poznámka**	
Authority Key Identifier			
Key Identifier		Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.	
Subject Key Identifier			
Subject Alternative Name			
dNSName	DNS název V certifikátu může být vloženo až 20 DNS názvů.	**povinné**	Certifikát musí obsahovat minimálně jeden záznam dNSName
Key Usage ***(kritické rozšíření)***			
DigitalSignature		Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.	
KeyEncipherment			
Extended Key Usage			
KeyPurposeID	id-kp-serverAuth	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.	
Certificate Policies			
Policy Information [1]			
Policy Identifier	OID této certifikační politiky	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.	
Policy Information [2]			

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

Policy Identifier	2.23.140.1.2.2 *organization-validated*	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit. Výjimkou jsou certifikáty vydané podnikající fyzické osobě, které tento identifikátor neobsahují.
CRL Distribution Points		
URI	http://crl.postsignum.cz/crl/pspublicca5.crl	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.
URI	http://crl2.postsignum.cz/crl/pspublicca5.crl	
URI	http://crl.postsignum.eu/crl/pspublicca5.crl	
AuthorityInfoAccess		
accessMethod URI	id-ad-caIssuers (1.3.6.1.5.5.7.48.2) http://crt.postsignum.cz/crt/pspublicca5.crt	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.
accessMethod URI	OCSP (1.3.6.1.5.5.7.48.1) http://ocsp.postsignum.cz/OCSP/VCA5/	
Signed Certificate Timestamp		
Položka je v souladu s RFC 6962 a obsahuje časovou značku a ID logů Certificate Transparency (CT log), ve kterých je obsažen vydaný precertifikát, který odpovídá vydanému doménovému certifikátu. Precertifikát je zasílán minimálně do 3 CT logů. Seznam CT logů, do kterých jsou precetifikáty zasílány, je uveden na webových stránkách poskytovatele.		

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

7.1.2.4 Profil OCSP

Entry name	Value / index
Version	3 (0x2)
Serial Number	sériové číslo certifikátu přidělené certifikační autoritou
SignatureAlgorithm	sha384WithRSAEncryption
Issuer	
C countryName	CZ
organizationIdentifier OID 2.5.4.97	NTRCZ-47114983
O organisationName	Česká pošta, s.p.
CN commonName	PostSignum Qualified CA 5
Validity	
Not Before	Počátek platnosti vydaného certifikátu (UTCTime)
Not After	Konec platnosti vydaného certifikátu (UTCTime)
Subject	
C countryName	CZ
organizationIdentifier OID 2.5.4.97	NTRCZ-47114983
O organisationName	Česká pošta, s.p.
OU organizationalUnitName	PostSignum Services
CN commonName	PostSignum VCA 5 - OCSP Responder X *(X je číslo označující konkrétního odpovídače OCSP)*
Subject Public Key Info	
Algorithm	rsaEncryption
SubjectPublicKey	*veřejný klíč odpovídače OCSP* *algoritmus RSA, velikost klíče alespoň 3072 bitů*
Extensions	*prodloužení certifikátu dle níže uvedené tabulky*
Signature	*elektronická pečeť poskytovatele certifikačních služeb*

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

Tab. 1 Rozšíření certifikátu:

Entry name	Value / index	Critical yes/no
Authority Key Identifier		Ne
Key Identifier	*Použito*	
Subject Key Identifier	*Použito*	Ne
Key Usage		Ano
DigitalSignature	Ano	
NonRepudiation	Ne	
KeyEncipherment	Ne	
DataEncipherment	Ne	
KeyAgreement	Ne	
KeyCertSign	Ne	
CRLSign	Ne	
Extended Key usage		Ne
KeyPurposeID	id-kp-OCSPSigning	
CertificatePolicies		Ne
Policy Information		
Policy Identifier	OID of this certification policy	
AuthorityInfoAccess		Ne
accessMethod URI	id-ad-caIssuers (1.3.6.1.5.5.7.48.2) http://crt.postsignum.cz/crt/pspublicca5.crt	
OCSP No Check	id-pkix-*ocsp-nocheck*	Ne

7.1.2.5 Všechny certifikáty

PostSignum VCA nevystaví certifikát, který obsahuje jiný příznak keyUsage, hodnotu extKeyUsage, rozšíření certifikátu nebo jiná data, která nejsou specifikována v kapitolách 7.1.2.1, 7.1.2.2 nebo 7.1.2.3. PostSignum VCA si vyhrazuje právo vložit do certifikátu položky na rámec uvedených profilů v případě změny technických norem.

7.1.3 Objektové identifikátory (dále „OID“) algoritmů

PostSignum VCA využívá následující algoritmy:

sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11) nebo
sha384WithRSAEncryption (OID 1.2.840.113549.1.1.12) pro certifikáty žadatelů
sha512WithRSAEncryption (OID 1.2.840.113549.1.1.13) pro certifikáty kořenové a podřízené autority

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. Položky v certifikátu nesmí obsahovat samostatně tyto znaky: ‘,‘ (čárka), ‘-’ (pomlčka) a ’ ’ (mezera).

FQDN v položce CN nebo SAN nesmí obsahovat znak ‘_‘ (podtržítko).

7.1.5 Omezení jmen a názvů

Žádná omezení „Name Constraints“ nejsou v PostSignum VCA aplikována.

7.1.6 OID certifikační politiky

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

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

Dále je v certifikátu uvedeno OID 2.23.140.1.2.2 (organization-validated) dle specifikace [CA/B] pro certifikáty s ověřenou identitou organizace.

V certifikátech kořenové a podřízené CA je uvedeno OID 2.5.29.32.0 (Any Policy).

7.1.7 Rozšiřující položka „Policy Constraints“

Rozšiřující položka „Policy Constraints“ se v PostSignum VCA 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.

7.1.9 Způsob zápisu kritické rozšiřující položky „Certificate Policies“

Způsob zápisu rozšiřující položky „Certificate Policies“ je uveden v kapitole 7.1.2.3. Tato položka není označena jako kritická.

7.2 Profil seznamu zneplatněných certifikátů

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 Public CA 5
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 tabulka níže
CrlExtensions	rozšíření CRL podle tabulky v kapitole 7.2.2
SignatureAlgorithm	sha384withrsaencryption
Signature	elektronická pečeť poskytovatele certifikačních služeb

7.2.1 Číslo verze

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

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

Rozšíření v CRL

Název rozšiřující položky	**Hodnota/příznak použití**	**Kritická ano/ne**

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

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

OCSP je v souladu s RFC 6960.

Struktura OCSP žádosti – OCSP Request Data

Název položky	Popis	Hodnota/příznak použití
Version	Verze protokolu OCSP (povinná položka)	1
Requestor List		
Certificate ID	údaje o dotazovaném certifikátu – položka se může opakovat	
Hash Algorithm	hash žádosti	SHA-1
Issuer Name Hash	hash vypočítaný ze jména vydavatele certifikátu	
Issuer Key Hash	hash vypočítaný z otisku veřejného klíče vydavatele certifikátu	
Serial Number	sériové číslo dotazovaného certifikátu	
Request Extensions		
OCSP Nonce	Náhodné, jednou vygenerované číslo (64 bitů). Je-li obsaženo v žádosti, pak ho obsahuje i odpověď. (nepovinná položka)	

Žádost OCSP nemusí být podepsaná.

Struktura OCSP odpovědi – OCSP Response Data

Název položky	Popis	Hodnota/příznak použití
OCSP Response Status	Přirozené číslo, označující stav odpovědi	0 – successful 1 – malformedRequest 2 – internalError 3 – tryLater 6 – unauthorized
Response Type	Basic OCSP Response	
Version	Verze protokolu OCSP	1
Responder Id	DN podpisového certifikátu OCSP serveru	
Produced At	Čas podpisu odpovědi OCSP serveru	
Responses:		
Certificate ID	Údaje odpovídají údajům v žádosti	
Cert Status	Stav certifikátu. good – certifikát je platný revoked – certifikát je zneplatněný unknown – stav certifikátu je neznámý (např. takový certifikát neexistuje)	0 – good 1 – revoked 2 – unknown

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

Revocation Time	Čas revokace certifikátu. Položka je uvedena pouze v případě Cert Status=revoked	
Revocation Reason	Důvod revokace certifikátu. Položka je uvedena pouze v případě Cert Status=revoked	CRLReason obsahuje hodnotu povolenou pro CRL, jak je uvedeno v kapitole 4.9.1.1.
This Update	Čas, od něhož je indikován stav odpovědi.	
Response Extensions		
OCSP Nonce	Náhodné, jednou vygenerované číslo (64 bitů). Je-li obsaženo v žádosti, pak ho obsahuje i odpověď. (nepovinná položka)	

7.3.1 Číslo verze

Verze protokolu OCSP je 1.

7.3.2 Rozšiřující položky OCSP

Rozšíření v žádosti a odpovědi OCSP je uvedeno v tabulkách v kapitole 7.3.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

8 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

V prostředí PostSignum VCA jsou pravidelně prováděny kontroly minimálně 1x za rok. Kontrolovaná období na sebe vždy navazují. 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.

Součástí kontroly je kontrola bezpečnostní shody.

8.2 Identita a kvalifikace auditora

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

Audit CA provádí kvalifikovaný auditor. Kvalifikovaný auditor znamená fyzickou osobu, právnickou osobu nebo skupinu fyzických osob či právnických osob, které společně disponují následujícími kvalifikacemi a dovednostmi:

1. Nezávislost na České poště, jakožto subjektu podléhajícímu auditu;

2. Schopnost provést audit, který splňuje kritéria uvedená ve schématu způsobilého auditu (viz oddíl 8.4);

3. Zaměstnává osoby, které mají odborné znalosti v oblasti zkoumání technologií infrastruktury veřejných klíčů, nástrojů a technik informační bezpečnosti, auditů informačních technologií a bezpečnosti a funkce ověřování třetí stranou;

4. Pro audity prováděné v souladu s kteroukoli z norem ETSI akreditovaných v souladu s normou ISO 17065 s použitím požadavků uvedených v normě ETSI EN 319 403;

5. Vázán zákonem, vládním nařízením nebo profesním etickým kodexem.

8.3 Vztah hodnotitele k hodnocenému subjektu

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

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

8.4 Hodnocené oblasti

8.5 Audit se provádí v souladu s normami [ETSI EN 319 401], [ETSI EN 319 411] (měla by být použita nejnovější verze odkazovaných dokumentů ETSI), část 1 – 3 v souladu s požadavky Mozilla a [CA/B] v aktuální verzi požadavků CCADB.Postup v případě zjištění nedostatků

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

V případě zjištění incidentu (např. chybně vydaný certifikát, obecně stavy, které jsou v rozporu s jakýmikoliv platnými standardy, kterými se tato certifikační politika řídí) je postupováno v souladu s požadavky uvedenými na wiki.mozilla (CA/Responding To An Incident).

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

8.6 Sdělování výsledků hodnocení

O provedení každé kontroly je vypracována podepsaná písemná zpráva v souladu s [CA/B] dle vzoru uvedeného na této webové stránce https://www.ccadb.org/policy#51-audit-statement-content. Zpráva je předána Manažerovi CA. Ten zajistí její distribuci a projednání.

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

Zprávu z kontroly zveřejňuje na svých webových stránkách auditní společnost.

8.7 Vlastní audity

V prostředí PostSignum VCA jsou pravidelně prováděny interní kontroly na náhodném vzorku (min. 3% z vydaných certifikátů) minimálně 1x za 3 měsíce.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

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 VCA 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 VCA tuto službu neposkytuje.

9.3 Citlivost obchodních informací

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

9.3.1 Výčet citlivých informací

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

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

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 komerčním certifikátu, pokud k jeho zveřejnění dal držitel souhlas.

9.3.3 Odpovědnost za ochranu citlivých informací

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

9.3.4 Poskytnutí citlivých informací pro soudní či správní účely

Veškeré informace zpracovávané v PostSignum VCA jsou zpřístupněny orgánům zmocněným ze zákona v případech, kdy to zákon vyžaduje, a do té míry, do jaké to zákon vyžaduje. Zpřístupnění informací zajistí Manažer 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 ustavení [GDPR], obecně závazných právních přepisů a interních předpisů České pošty upravujících problematiku ochrany osobních údajů.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

9.5 Práva duševního vlastnictví

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

Je povolena distribuce a reprodukce tohoto dokumentu pouze v plném rozsahu.

9.6 Zastupování a záruky

9.6.1 Zastupování a záruky CA

Česká pošta zaručuje, že splní veškeré povinnosti uložené touto certifikační politikou a ustanoveními příslušných právních předpisů a norem, především [CA/B].

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

9.6.2 Zastupování a záruky RA

V poskytování služeb registrační autority nemůže být Česká pošta jako poskytovatel certifikačních služeb zastupována třetím subjektem.

9.6.3 Zastupování a záruky držitele certifikátu

Zákazník (držitel certifikátu) nebo žadatel ručí za naplnění všech povinnosti zákazníků a žadatelů o certifikát uvedených v této certifikační politice. Více informací je k dispozici v kapitolách 4.1.2.3 a 4.1.2.5.

9.6.4 Zastupování a záruky spoléhajících se stran

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

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

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

9.7 Zřeknutí se záruk

Záruky uvedené v kapitole 0 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.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

9.8 Omezení odpovědnosti

Česká pošta neodpovídá za škodu vyplývající z použití komerčního 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 komerčního certifikátu v období po přijetí žádosti o jeho zneplatnění, pokud Česká pošta dodrží lhůtu pro zveřejnění zneplatněného komerčního certifikátu na seznamu zneplatněných certifikátů (CRL), uvedenou v kapitole 0 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. 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 směrovaným 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.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

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

9.11.2 Komunikace v rámci systému PostSignum VCA

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

9.11.3 Komunikační jazyk

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

9.12 Změny

9.12.1 Postup při změnách

Postupy pro zapracování změn jsou uvedeny v 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] 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 VCA. 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 VCA.

OID jsou přiřazeny:

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

OID nejsou přiřazeny registračním autoritám ani certifikační prováděcí směrnici.

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.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

9.13 Řešení sporů

V případě vzniku sporu mezi zákazníkem a PostSignum VCA 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 VCA řešit u místně a věcně příslušného soudu.

9.14 Rozhodné právo

Činnost PostSignum VCA se řídí právním řádem České republiky.

9.15 Shoda s právními předpisy

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

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

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.

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.

Pokud dojde k rozporu mezi touto certifikační politikou a [CA/B], platí ustanovení [CA/B].

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.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.

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:

[CA/B]	CA/Browser Forum - Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates
[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 6962]	Certificate Transparency
[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
[ZoSVD]	Zákon č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce v platném znění

9.17.2 Odkazy a literatura

[VOP]	Všeobecné obchodní podmínky certifikačních služeb.

Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.