Politika PostSignum Qualified CA pro vydávání kvalifikovaných prostředků pro vytváření elektronických podpisů

Verze 1.0

OBSAH

Evidence revizí a změn

Verze	Účinnost od	Důvod a popis změny	Autor	Schválil
1.0	10. 10. 2016	Upravená politika pro vydávání SSCD prostředků	Trávníček	PAA

1 ÚVOD

Tento dokument stanoví pravidla a postupy pro vydávání kvalifikovaných prostředků pro vytváření elektronických podpisů.

1.1 Přehled

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

Kromě služeb vydávání kvalifikovaných certifikátů pro elektronický podpis a certifikátů pro elektronickou pečeť nabízí PostSignum QCA zákazníkům službu vydávání kvalifikovaných prostředků pro vytváření elektronických podpisů.

Prostředky vydávané podle této politiky jsou kvalifikované prostředky pro vytváření elektronických podpisů podle Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 (eIDAS).

Kvalifikované prostředky pro vytváření elektronických podpisů vydávané podle této politiky zajišťují generování klíčového materiálu a vytváření elektronických podpisů uvnitř vlastního hardware prostředku a poskytují ochranu úložiště klíčového materiálu komplexní hodnotou PIN. PostSignum QCA se samotným kvalifikovaným prostředkem pro vytváření elektronických podpisů dodává i ovladače pro instalaci do běžných OS a aplikaci umožňující správu a obsluhu prostředku a generování klíčových párů a žádostí o certifikát.

Vydávání kvalifikovaných prostředků pro vytváření elektronických podpisů není vázáno na uzavření smlouvy o poskytování certifikačních služeb, prostředky si může od České pošty zakoupit i fyzická nebo právnická osoba, která do té doby nebyla zákazníkem PostSignum QCA.

Tato politika se zabývá správou kvalifikovaných prostředků pro vytváření elektronických podpisů na straně PostSignum QCA a stanovuje podmínky pro práci s prostředky na straně jejich držitele.

1.2 Název a jednoznačné určení dokumentu

Tab. 1 Identifikace politiky

Název dokumentu	Politika PostSignum Qualified CA pro vydávání kvalifikovaných prostředků pro vytváření elektronických podpisů
Verze dokumentu	1.0
Stav	Finální
OID poskytovatele certifikačních služeb	2.23.134
OID PostSignum Root QCA	2.23.134.1.4.2.1
OID PostSignum Qualified CA	2.23.134.1.4.2.2
OID této politiky	2.23.134.1.4.1.200.100
Datum vydání	7. 10. 2016
Doba platnosti	Do odvolání nebo do dne ukončení služeb autorit PostSignum QCA.

1.3 Participující subjekty

Kvalifikované prostředky pro vytváření elektronických podpisů podle této politiky mohou být vydávány pouze Českou poštou.

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.: 267 196 111

e-mail: info@cpost.cz

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

1.3.1 Distribuční místa kvalifikovaných prostředků pro vytváření elektronických podpisů

Distribuce kvalifikovaných prostředků pro vytváření elektronických podpisů je zajišťována prostřednictvím PostShopu České pošty dostupným na webových stránkách https://www.postshop.cz nebo jiným distribučním kanálem České pošty.

1.3.2 Držitelé kvalifikovaných prostředků pro vytváření elektronických podpisů

Držitelem kvalifikovaného prostředku pro vytváření elektronických podpisů je libovolná fyzická nebo právnická osoba, která tento prostředek zakoupila od České pošty.

1.3.3 Jiné participující subjekty

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

1.4 Použití kvalifikovaného prostředku pro vytváření elektronických podpisů

1.4.1 Přípustné použití kvalifikovaného prostředku pro vytváření elektronických podpisů

Kvalifikované prostředky pro vytváření elektronických podpisů vydané podle této politiky jsou určeny pro generování klíčových párů a vytváření elektronických podpisů založených na certifikátech vydaných PostSignum QCA.

Seznam podporovaných kvalifikovaných prostředků pro vytváření elektronických podpisů je uveden na webových stránkách poskytovatele.

1.4.2 Omezení použití kvalifikovaného prostředku pro vytváření elektronických podpisů

Kvalifikované prostředky pro vytváření elektronických podpisů vydané podle této 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 tuto politiku nebo certifikační prováděcí směrnici

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

1.5.2 Kontaktní osoba organizace spravující tuto politiku nebo certifikační prováděcí směrnici

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

manager.postsignum@cpost.cz

nebo na webových stránkách poskytovatele.

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

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

1.5.4 Postupy při schvalování souladu podle 1.5.3

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

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

1.6 Přehled použitých pojmů a zkratek

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

Certifikát pro elektronickou pečeť – certifikát vydaný v souladu s [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.

Elektronické časové razítko – časové razítko ve smyslu [eIDAS].

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

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

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

Kvalifikovaný prostředek pro vytváření elektronických podpisů – HW zařízení (USB token nebo čipová karta), které splňuje požadavky [eIDAS] na vytváření kvalifikovaného elektronického podpisu.

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.

Pečetící osoba – osoba definovaná [eIDAS].

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

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 kvalifikovaný systémový certifikát.

PostSignum QCA – hierarchie certifikačních autorit, vydávajících kvalifikované certifikáty pro elektronický podpis a certifikáty pro elektronickou pečeť ve smyslu [eIDAS].

PostSignum VCA – hierarchie certifikačních autorit, vydávajících komerční certifikáty.

PostSignum Root QCA – kořenová certifikační autorita, která má samopodepsaný kvalifikovaný systémový certifikát. Vydala kvalifikované systémové certifikáty pro podřízené certifikační autority a CRL. V hierarchii PostSignum mohou existovat další kořenové certifikační autority, které jsou navíc označeny pořadovým číslem, např. PostSignum Root QCA 2.

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

PostSignum Public CA – certifikační autorita, která má kvalifikovaný systémový certifikát 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 elektronická časová razítka ve smyslu [eIDAS]. Autoritu tvoří více jednotek (TSU). Každá jednotka má vlastní klíč a kvalifikovaný systémový certifikát.

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.

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

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

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

Uživatel certifikátu (relying party) – osoba, která užívá certifikát vydaný PostSignum například pro ověření elektronického podpisu, značky 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 značek, dat pro ověřování elektronických pečetí a dat pro šifrování.

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

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

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, pečetící osobu a označující fyzickou osobu.

2 ODPOVĚDNOST ZA ZVEŘEJŇOVÁNÍ A ÚLOŽIŠTĚ INFORMACÍ A DOKUMENTACE

2.1 Úložiště informací a dokumentace

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

Jedinou výjimkou je úložiště na adrese postsignum.ttc.cz provozované společností TTC Telekomunikace, s.r.o.

Za zveřejňování informací odpovídá Česká pošta jako poskytovatel certifikačních služeb.

2.2 Zveřejňování informací a dokumentace

Česká pošta nezveřejňuje informace o vydaných kvalifikovaných prostředcích pro vytváření elektronických podpisů.

2.2.1 Zveřejňování informací o certifikační autoritě

Certifikační politiky, zpráva pro uživatele, návod na použití kvalifikovaných prostředků pro vytváření elektronických podpisů a případně i další dokumenty jsou zveřejňovány na

- webových stránkách poskytovatele, nebo
- obchodních místech (pouze k nahlédnutí).

Další důležité informace, zejména informace požadované [eIDAS] (např. informace o změně bezpečnostních parametrů prostředku, odnětí akreditace) 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 (konkrétně deníku Hospodářské noviny).

2.3 Periodicita zveřejňování informací

Informace jsou zveřejňovány v následujících intervalech:

- certifikační politiky, certifikační prováděcí směrnice, zpráva pro uživatele a návody jsou zveřejňovány po schválení a vydání nové verze,
- důležité informace, zejména informace požadované [eIDAS] jsou zveřejňovány neprodleně.

2.4 Řízení přístupu k jednotlivým typům úložišť

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

3 IDENTIFIKACE A AUTENTIZACE

PostSignum QCA neprovádí identifikaci ani autentizaci zákazníků, kteří se chtějí stát držiteli kvalifikovaných prostředků pro vytváření elektronických podpisů.

Ověření žadatele při vydání certifikátu se řídí příslušnou certifikační politikou.

Ověření toho, že klíčový pár byl generován v kvalifikovaném prostředku pro vytváření elektronických podpisů, je prováděno pomocí klíčového páru pro autentizaci tzv. „servisní klíč“, jehož vytvoření se řídí ustanovením v kapitole 4.2.

Pokud na prostředku nebude v době vytváření žádosti o prvotní nebo následný certifikát servisní klíč přítomen (např. dojde k jeho výmazu), nebude možné tento prostředek použít pro vytvoření žádosti o prvotní nebo následný certifikát.

Při vydání prvotního certifikátu dochází k vytvoření vazby *prostředek–žadatel o certifikát*, která je kontrolována při vydávání dalších (následných) certifikátů, jejichž soukromý klíč byl vygenerován v prostředku.

3.1 Kritéria pro interoperabilitu

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

4 ŽIVOTNÍ CYKLUS KVALIFIKOVANÉHO PROSTŘEDKU PRO VYTVÁŘENÍ ELEKTRONICKÝCH PODPISŮ

4.1 Získání kvalifikovaného prostředku pro vytváření elektronických podpisů od dodavatele

Kvalifikované prostředky pro vytváření elektronických podpisů nakupuje Česká pošta od dodavatelů v souladu s interními předpisy České pošty.

4.2 Příprava prostředku pro zákazníka

Kvalifikovaný prostředek pro vytváření elektronických podpisů je České poště od dodavatele doručen v inicializovaném stavu, jsou na něm přednastaveny defaultní hodnoty PIN a PUK.

Před vlastním předáním kvalifikovaného prostředku pro vytváření elektronických podpisů zákazníkovi provádí PostSignum QCA následující kroky:

- přečtení a záznam vnitřního sériového čísla prostředku,
- vygenerování klíčového páru pro autentizaci prostředku ke službám PostSignum QCA tzv. "servisního klíče".

4.3 Vydání prostředku

4.3.1 Subjekty oprávněné žádat o vydání kvalifikovaného prostředku pro vytváření elektronických podpisů

Oprávnění žádat o kvalifikovaný prostředek pro vytváření elektronických podpisů má jakákoliv fyzická nebo právnická osoba.

4.3.2 Uzavření smlouvy

Vydání kvalifikovaného prostředku pro vytváření elektronických podpisů není vázáno na uzavření smlouvy o poskytování certifikačních služeb s Českou poštou.

4.3.3 Odpovědnost poskytovatele

Poskytovatel certifikačních služeb je při vydávání a správě kvalifikovaných prostředků pro vytváření elektronických podpisů zejména povinen:

- před předáním zákazníkovi uchovávat kvalifikované prostředky pro vytváření elektronických podpisů tak, aby nemohlo dojít k jejich zneužití třetí osobou,
- před předáním zákazníkovi uchovávat kvalifikované prostředky pro vytváření elektronických podpisů tak, aby nemohlo dojít k jejich poškození vlivem vnějšího prostředí,
- vydat kvalifikovaný prostředek pro vytváření elektronických podpisů nepoškozený a v definovaném stavu (viz kapitola 4.2),
- zveřejňovat certifikační politiky, podle kterých vydává kvalifikované prostředky pro vytváření elektronických podpisů, na webových stránkách poskytovatele, případně jinými vhodnými způsoby (viz kapitola 2.2),
- zveřejnit návod pro použití kvalifikovaného prostředku pro vytváření elektronických podpisů,
- poskytnout držitelům kvalifikovaných prostředků pro vytváření elektronických podpisů nástroj pro generování klíčových párů v prostředku,

- 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.

4.4 Převzetí kvalifikovaného prostředku pro vytváření elektronických podpisů

Převzetí kvalifikovaného prostředku pro vytváření elektronických podpisů je možné

- osobně prostřednictvím PostShopu České pošty;
- prostřednictvím dalších služeb České pošty v souladu s obchodními podmínkami PostShopu České pošty,
- jiným způsobem po vzájemné dohodě.

Současně s kvalifikovaným prostředkem pro vytváření elektronických podpisů přebírá žadatel i instalační software pro zajištění komunikace s prostředkem. Instalační software je žadateli předán v elektronické formě závislé na způsobu doručení prostředku.

4.4.1 Úkony spojené s převzetím kvalifikovaného prostředku pro vytváření elektronických podpisů a odpovědnost držitele

Poté, co zákazník obdrží kvalifikovaný prostředek pro vytváření elektronických podpisů, zkontroluje, že prostředek nevykazuje znaky poškození vlivem uskladnění nebo manipulace s ním. Pokud prostředek takové znaky vykazuje, kontaktuje žadatel Českou poštu, která věc řeší v souladu s reklamačním řádem.

Převzetím kvalifikovaného prostředku pro vytváření elektronických podpisů se zákazník stává držitelem prostředku. Zároveň stvrzuje, že na sebe bere závazky vyplývající z politiky, podle které byl prostředek vydán.

Držitel kvalifikovaného prostředku pro vytváření elektronických podpisů je dále povinen zejména:

- seznámit se s politikou, podle které mu byl prostředek vydán,
- změnit přednastavený PIN chránící přístup ke klíčovým párům generovaným a uloženým v prostředku při prvním použití prostředku,
- po instalaci obslužných programů zkontrolovat, že prostředek nevykazuje znaky možného dřívějšího použití nad rámec kapitoly 4.2 (zkontroluje obsah prostředku). Pokud prostředek takové znaky vykazuje, kontaktuje žadatel Českou poštu, která věc řeší v souladu s reklamačním řádem,
- využívat kvalifikované prostředky pro vytváření elektronických podpisů pouze v souvislosti s řádnými a legálními účely a v souladu s platnými právními předpisy.

4.4.2 Zveřejňování vydaných kvalifikovaných prostředků pro vytváření elektronických podpisů poskytovatelem

PostSignum QCA nezveřejňuje informace o vydaných kvalifikovaných prostředcích pro vytváření elektronických podpisů.

4.4.3 Oznámení o vydání prostředku jiným subjektům

Poskytovatel certifikačních služeb neoznamuje vydání prostředku žádné třetí straně.

4.5 Použití kvalifikovaného prostředku pro vytváření elektronických podpisů

Držitel kvalifikovaného prostředku pro vytváření elektronických podpisů:

- nakládá s prostředkem s náležitou péčí, a to tak, aby nemohlo dojít k jeho zneužití,
- pokud jsou na prostředku generována a uložena párová data pro vytváření a ověřování elektronických podpisů, nakládá držitel s prostředkem tak, aby byla párová data chráněna v souladu s požadavky certifikační politiky, podle které byla generována.

V případě ztráty nebo odcizení prostředku neposkytuje PostSignum QCA náhradní prostředek.

4.5.1 Generování párových dat na prostředku

PostSignum QCA poskytuje držitelům kvalifikovaných prostředků pro vytváření elektronických podpisů nástroje umožňující generování a správu párových dat v prostředku. PostSignum QCA neposkytuje žádné záruky dané touto politikou v případě použití jiných nástrojů.

4.6 Obnovení kvalifikovaného prostředku pro vytváření elektronických podpisů

Česká pošta neposkytuje služby obnovení kvalifikovaného prostředku pro vytváření elektronických podpisů v případě ukončení jejich životnosti.

4.6.1.1 Pozastavení nebo ukončení vydávání kvalifikovaného prostředku pro vytváření elektronických podpisů

V případě, že se objeví podezření na oslabení kryptografických nebo jiných bezpečnostních parametrů prostředku, je PostSignum QCA oprávněna pozastavit nebo zcela zrušit vydávání prostředků. V tomto případě PostSignum QCA upozorní držitele prostředků na nastalou situaci neprodleně poté, co tuto informaci obdrží a ověří. Upozornění bude zveřejněno na webových stránkách poskytovatele.

4.6.2 Dostupnost služeb

Služba vydávání kvalifikovaných prostředků pro vytváření elektronických podpisů je dostupná při objednávání prostředků přes PostShop České pošty v souladu s obchodními podmínkami PostShopu, případně jiným způsobem po vzájemné dohodě.

5 MANAGEMENT, PROVOZNÍ A FYZICKÁ BEZPEČNOST

Pro PostSignum QCA byly zpracovány dokumenty:

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

Zmíněné dokumenty byly vypracovány na základě výsledků provedené analýzy rizik.

Tyto dokumenty jsou mj. přístupné osobám, které provádějí kontrolu bezpečnostní shody PostSignum QCA. Tato kapitola vychází z výše uvedených dokumentů a poskytuje stručný přehled základních bezpečnostních zásad uplatňovaných v PostSignum QCA, týkající se vydávání kvalifikovaných prostředků pro vytváření elektronických podpisů.

5.1 Fyzická bezpečnost

5.1.1 Uložení kvalifikovaných prostředků pro vytváření elektronických podpisů u poskytovatele

Prostředky jsou uloženy v centrálním skladu Praha tak, aby byly chráněny proti vlivům prostředí (vlhkost, mechanické poškození).

5.1.2 Fyzický přístup k prostředkům

Do skladových pracovišť centrálního skladu Praha mají fyzický přístup výhradně pracovníci centrálního skladu Praha, ostatní osoby pouze v doprovodu. Prostory jsou chráněny proti neoprávněnému vniknutí mechanickými prostředky (bezpečnostní zámek).

5.1.3 Vlivy vody

Prostředky jsou uloženy v centrálním skladu Praha tak, že vliv vody je eliminován.

5.1.4 Protipožární opatření a ochrana

Prostory centrálního skladu Praha jsou vybaveny elektronickou požární signalizací (EPS).

5.2 Procesní bezpečnost

5.2.1 Důvěryhodné role

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

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

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

Pro zajištění činností souvisejících s manipulací s kvalifikovanými prostředky pro vytváření elektronických podpisů není požadována přítomnost více osob.

5.2.3 Identifikace a autentizace pro každou roli

Ke kvalifikovanému prostředku pro vytváření elektronických podpisů pracovník PostSignum QCA s oprávněním k přípravě prostředku pro zákazníka autentizuje zadáním PIN.

5.2.4 Role vyžadující rozdělení povinností

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

Vzhledem k procesům vydávání kvalifikovaných prostředků pro vytváření elektronických podpisů není požadována žádná další separace rolí nad rámec dokumentu Organizační zajištění úlohy Kvalifikovaná certifikační autorita České pošty, s.p.

5.3 Personální bezpečnost

5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

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

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

5.3.2 Posouzení spolehlivosti osob

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

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

5.3.3 Požadavky na přípravu pro výkon role, vstupní školení

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

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

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

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

5.3.4 Požadavky a periodicita školení

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

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

5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Požadavky na rotaci pracovníků a její frekvenci nejsou definovány.

5.3.6 Postihy za neoprávněné činnosti zaměstnanců

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

5.4 Auditní záznamy (logy)

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

5.4.1 Typy zaznamenávaných událostí

V PostSignum QCA jsou zaznamenávány následující události související se správou a distribucí kvalifikovaných prostředků pro vytváření elektronických podpisů:

Provozní záznamy:

- přijetí prostředků od dodavatele,
- vyskladnění prostředku za účelem jeho dodání zákazníkovi.

Auditní záznamy:

- získání vnitřního sériového čísla prostředku,
- generování klíčového páru pro autentizaci prostředku.

5.4.2 Periodicita zpracování záznamů

Auditní záznamy 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 v archivačním systému.

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 v archivačním systému.

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

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

5.4.7 Postup při oznamování události subjektu, který ji způsobil

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

5.4.8 Hodnocení zranitelnosti

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

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

5.5 Uchovávání informací a dokumentace

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

5.5.1 Typy informací a dokumentace, které se uchovávají

V PostSignum QCA se v souvislosti s vydáváním kvalifikovaných prostředků pro vytváření elektronických podpisů uchovávají následující informace:

- obslužný software pro zajištění komunikace s prostředky (middleware)
- dokumentace související s vydáváním kvalifikovaných prostředků pro vytváření elektronických podpisů (zejména tato politika a uživatelská příručka)

5.5.2 Doba uchování uchovávaných informací a dokumentace

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

5.5.3 Ochrana úložiště uchovávaných informací a dokumentace

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

5.5.4 Postupy při zálohování uchovávaných informací a dokumentace

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

5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

V souvislosti s vydáváním kvalifikovaných prostředků pro vytváření elektronických podpisů není používání časových razítek vyžadováno.

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

V prostředí PostSignum QCA jsou auditní záznamy shromažďovány a přesouvány do archivního systému 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 Obnova po havárii nebo kompromitaci

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

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

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

5.6.1 Postup v případě incidentu a kompromitace

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

5.6.2 Poškození výpočetních prostředků, softwaru nebo dat

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

5.7 Ukončení činnosti poskytovatele certifikačních služeb

Činnost poskytovatele certifikačních služeb bude ukončena v souladu s platnými právními předpisy.

5.8 Odnětí akreditace

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

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

6 TECHNICKÁ BEZPEČNOST

6.1 Technické parametry kvalifikovaného prostředku pro vytváření elektronických podpisů

Technické parametry kvalifikovaného prostředku pro vytváření elektronických podpisů jsou dostupné v technické dokumentaci, která je ke stažení z webových stránek poskytovatele.

Technické parametry prostředku zaručují, že ho lze použít v operačních systémech uvedených v technické dokumentaci. Podporované kryptografické algoritmy a délky klíčů umožňují použití prostředku pro generování a ukládání klíčových párů v souladu s certifikačními politikami PostSignum

6.2 Generování a instalace párových dat

PostSignum QCA poskytuje držitelům kvalifikovaných prostředků pro vytváření elektronických podpisů aplikaci umožňující generování klíčových párů uvnitř prostředku. Tato aplikace je k dispozici pro operační systémy rodiny Microsoft Windows a je možné ji použít pouze v režimu online. Aplikace je zdarma ke stažení na webu poskytovatele.

Kvalifikovaný prostředek pro vytváření elektronických podpisů neumožňuje export soukromého klíče vygenerovaného v prostředku.

Přístup ke klíčovým párům generovaným a uloženým v kvalifikovaném prostředku pro vytváření elektronických podpisů je chráněn pomocí PIN.

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

Veřejný klíč žadatele je poskytovateli certifikačních služeb doručen v elektronické podobě, v žádosti o certifikát ve formátu PKCS#10. Aplikace poskytovaná PostSignum QCA umožňuje vytvoření a odeslání PKCS#10 žádosti ke zpracování v PostSignum QCA.

6.2.2 Délky párových dat

V prostředí PostSignum QCA jsou pro vydávání certifikátů podporovány klíče pro algoritmus RSA s délkou modulu 2048 nebo 4096 bitů.

V prostředí PostSignum QCA nejsou pro vytváření a ověřování elektronických podpisů podporovány jiné algoritmy.

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

Generování klíčového materiálu je prováděno uvnitř kvalifikovaného prostředku pro vytváření elektronických podpisů, kvalita vygenerovaného materiálu je ověřována nástroji prostředku.

V případě žádosti o certifikát u certifikační autority PostSignum je kontrola kvality dat pro ověřování elektronických podpisů nastavena na úrovni certifikační autority, která kontroluje jedinečnost a povolenou délku veřejného klíče.

6.2.4 Postup při zničení dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí

Klíčový materiál vygenerovaný a uložený uvnitř prostředku je možné smazat z přístupného uživatelského rozhraní po zadání PIN pro přístup k úložišti klíčů. Je při tom nutné dbát na to, aby nedošlo k odstranění klíčového páru pro autentizaci, tzv. „servisního klíče“.

V případě odstranění klíčového páru pro autentizaci „servisního klíče“ nebude možné prostředek použít pro vytvoření žádosti o certifikát. Postup pro obnovení klíčového páru pro autentizaci je následující:

- z prostředku odstranit veškeré klíčové páry včetně certifikátů pomocí uživatelského rozhraní,
- změnit hodnotu PIN na defaultní hodnotu uvedenou v dokumentaci k prostředku,
- zaslat prostředek na adresu uvedenou v dokumentaci k prostředku.

6.2.5 Hodnocení kvalifikovaných prostředků pro vytváření elektronických podpisů

PostSignum QCA vydává prostředek, který je kvalifikovaným prostředkem pro vytváření elektronických podpisů dle [eIDAS]. Nepředpokládá se tedy, 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.

7 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

7.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

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

7.2 Identita a kvalifikace hodnotitele

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

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

7.3 Vztah hodnotitele k hodnocenému subjektu

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

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

7.4 Hodnocené oblasti

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

7.5 Postup v případě zjištění nedostatků

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

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

7.6 Sdělování výsledků hodnocení

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

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

8 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

8.1 Poplatky

8.1.1 Poplatky za vydání kvalifikovaného prostředku pro vytváření elektronických podpisů

Cena je stanovena na webových stránkách PostShopu České pošty a může být zahrnuta i v ceně jiné služby poskytované Českou poštou.

8.1.2 Poplatky za další služby

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

8.2 Finanční odpovědnost

8.2.1 Krytí pojištěním

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

8.2.2 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).

8.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

PostSignum QCA tuto službu neposkytuje.

8.3 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.

8.3.1 Výčet citlivých informací

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

8.3.2 Informace mimo rámec citlivých informací

Za důvěrné se nepovažují informace, které:

- se staly veřejně známými, aniž by to zavinila záměrně či opomenutím přijímající strana,
- měla přijímající strana legálně k dispozici před uzavřením smlouvy o poskytování certifikačních služeb, pokud takové informace nebyly předmětem jiné, dříve mezi zúčastněnými stranami uzavřené smlouvy o ochraně informací, nebo pokud takové informace nemají samy o sobě charakter obchodního tajemství,
- jsou výsledkem postupu, při kterém k nim přijímající strana dospěje nezávisle a je schopna to doložit svými záznamy nebo důvěrnými informacemi třetí strany,

- po uzavření smlouvy o poskytování certifikačních služeb poskytne přijímající straně třetí osoba, jež takové informace přitom nezíská přímo ani nepřímo od strany, jež je jejich vlastníkem, nebo je nezíská nezákonným způsobem, o čemž by přijímající strana věděla nebo vědět musela,

- jsou uvedené v kvalifikovaném certifikátu, pokud k jeho zveřejnění dal držitel souhlas.

8.3.3 Odpovědnost za ochranu citlivých informací

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

8.4 Ochrana osobních údajů

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

8.4.1 Politika ochrany osobních údajů

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

8.4.2 Osobní údaje

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

8.4.3 Údaje, které nejsou považovány za citlivé

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

8.4.4 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 [Z101].

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

Žadatel o kvalifikovaný prostředek pro vytváření elektronických podpisů dává České poště souhlas se zpracováním osobních údajů získaných během procesu nákupu a distribuce prostředku.

8.4.6 Poskytnutí citlivých informací pro soudní či správní účely

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

8.4.7 Jiné okolnosti zpřístupňování osobních údajů

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

8.5 Práva duševního vlastnictví

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

8.6 Zastupování a záruky

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

8.6.1 Zastupování a záruky RA

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

Jinak viz ustanovení kapitoly 8.6.

8.6.2 Zastupování a záruky držitele prostředku

Držitel kvalifikovaného prostředku pro vytváření elektronických podpisů ručí za naplnění všech povinnosti uvedených v této politice.

8.6.3 Zastupování a záruky ostatních zúčastněných subjektů

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

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

8.7 Zřeknutí se záruk

Záruky uvedené v kapitole 8.6 výše jsou výlučnými zárukami České pošty a Česká pošta jiné záruky neposkytuje.

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

8.8 Omezení odpovědnosti

Česká pošta neodpovídá za škodu vyplývající z použití kvalifikovaného prostředku pro vytváření elektronických podpisů, pokud došlo ze strany držitele k nedodržení omezení pro jeho použití, uvedených v této politice a zveřejněných na webové stránce poskytovatele.

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 politiky.

8.9 Odpovědnost za škodu, náhrada škody

Pokud nevyplývá z ustanovení platných právních předpisů jinak, odpovídá Česká pošta držiteli kvalifikovaného prostředku pro vytváření elektronických podpisů za škodu způsobenou porušením povinností České pošty uvedených v této politice.

8.10 Doba platnosti, ukončení platnosti

8.10.1 Doba platnosti

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

8.10.2 Ukončení platnosti

Platnost dokumentu je ukončena v případě

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

8.10.3 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 8, která se týkají obchodních a právních záležitostí.

8.11 Komunikace mezi zúčastněnými subjekty

8.11.1 Komunikace s poskytovatelem certifikačních služeb

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

Držitel kvalifikovaného prostředku pro vytváření elektronických podpisů komunikuje s poskytovatelem certifikačních služeb osobně. Obrací se na pracoviště registrační autority nebo na obchodní místa CA.

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

8.11.2 Komunikace v rámci systému PostSignum QCA

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

8.11.3 Komunikační jazyk

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

8.12 Změny

8.12.1 Postup při změnách

Postupy pro zapracování změn jsou uvedeny v kapitole. 1.5.

8.12.2 Postup při oznamování změn

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

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

V případě identifikace oslabení záruk poskytovaných použitím kvalifikovaného prostředku pro vytváření elektronických podpisů bude toto oznámeno na webových stránkách poskytovatele. Na toto oznámení mohou navazovat další akce, které jsou popsány v této certifikační politice.

8.12.3 Okolnosti, při kterých musí být změněn OID

Česká pošta přiřadila dle svých interních pravidel identifikátory objektů (OID) užívané v prostředí PostSignum QCA.

OID jsou přiřazeny:

- PostSignum Root QCA,
- každé certifikační autoritě, které PostSignum Root QCA vydala certifikát, zejména certifikační autoritě PostSignum Qualified CA,
- každé certifikační politice, podle které jsou vydávány certifikáty v rámci PostSignum QCA,
- každé politice pro vydávání kvalifikovaných prostředků pro vytváření elektronických podpisů.

OID nejsou přiřazeny registračním autoritám ani certifikační prováděcí směrnici.

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

8.13 Řešení sporů

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

Pokud Manažer CA nesjedná ukončení sporu, bude se spor mezi zákazníkem a PostSignum QCA řešit u místně a věcně příslušného soudu.

8.14 Rozhodné právo

Činnost PostSignum QCA se řídí právním řádem České republiky.

8.15 Shoda s právními předpisy

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

8.16 Další ustanovení

8.16.1 Rámcová dohoda

Žádná ustanovení v této kapitole.

8.16.2 Postoupení práv

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

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

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

8.16.3 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.

8.17 Další opatření

8.17.1 Řídící dokumenty

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

[CWA 141671]	CWA 14167-1:2003: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements
[eIDAS]	NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ESETSI EN 119 312Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI EN 319 411	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1 – 3
ETSI EN 319 412	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1 – 5

[ISO 27001]	ČSN ISO/IEC 27001:2014 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky
[ISO 27002]	ČSN ISO/IEC 27002:2014 Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací
[TS 101456]	ČSN ETSI TS 101 456 Elektronické podpisy a infrastruktury; Požadavky na postupy certifikační autority vydávající kvalifikované certifikáty, verze 1.3.1
[RFC 2511]	RFC 2511 – Internet X.509 Certificate Request Message Format
[RFC 3280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[RFC 5280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[RFC 3647]	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[RFC 3739]	Internet X.509 Public Key Infrastructure: Qualified Certificates Profile
[Z101]	Zákon č. 101/2000 Sb. o ochraně osobních údajů v aktuálním znění

8.17.2 Odkazy a literatura

[VOP]	Všeobecné obchodní podmínky certifikačních služeb