Certifikační autorita PostSignum QCA České pošty, s.p.

Certifikační politika PostSignum Root QCA

Verze 1.15

5. dubna 2005

Česká pošta, s.p.

Schváleno:

Verze	Schválil	
1.00	Komise pro certifikační politiky	e-mail: paa.postsignum@cpost.cz
1.15	Komise pro certifikační politiky	e-mail: paa.postsignum@cpost.cz

1. ÚVOD

1.1 Upozornění pro uživatele certifikátu

Před použitím certifikátu vydaného podle této certifikační politiky pozorně pročtěte tento dokument a ujistěte se, že jste mu řádně porozuměli.

1.2 Přehled

Česká pošta, s.p. (dále i ČP či Česká pošta) ustavila dvouúrovňovou hierarchii certifikačních autorit s názvem PostSignum QCA. Tato certifikační politika popisuje pravidla, podle kterých vydává certifikáty kořenová certifikační autorita PostSignum Root QCA.

Certifikáty vydané podle této politiky jsou kvalifikované systémové certifikáty ve smyslu zákona o elektronickém podpisu [ZoEP]. Jsou vydávány podřízeným certifikačním autoritám, které jsou provozovány v rámci PostSignum QCA České pošty.

Certifikační autorita, které byl vydán certifikát podle této certifikační politiky, musí být provozována Českou poštou, s.p.

Držiteli certifikátů vydaných PostSignum Root QCA jsou tedy certifikační autority provozované Českou poštou, které vydávají certifikáty dalším subjektům, jež však již nejsou certifikačními autoritami.

Soukromý klíč odpovídající veřejnému klíči v certifikátu vydaném autoritou PostSignum Root QCA je určen:

- k podpisu certifikátů subjektů, které nejsou certifikačními autoritami,
- k podpisu seznamu zneplatněných certifikátů (Certificate Revocation List - CRL).

Pravidla pro vydávání a správu kvalifikovaných systémových certifikátů podle této politiky jsou dále popsána v Certifikační prováděcí směrnici PostSignum QCA České pošty, verze 1.25, vydané dne 5.4.2005.

1.2.1 Certifikační služby poskytované PostSignum Root QCA

Certifikační autorita PostSignum Root QCA nabízí tyto certifikační služby:

- vydání certifikátu podle existujících certifikačních politik,
- revokace certifikátu, vydání CRL a jeho zveřejnění,
- informace o stavu certifikátu,
- informace o vydaných certifikátech,
- informace o poskytovaných službách.

1.3 Identifikace politiky

Tab. 1 Identifikace politiky

Název politiky	Certifikační politika PostSignum Root QCA
Verze politiky	1.15
Stav	finální

OID poskytovatele certifikačních služeb	2.23.134
OID PostSignum Root QCA	2.23.134.1.4.2.1
OID této politiky	2.23.134.1.4.1.4.115
Datum vydání	5.4.2005
Doba platnosti	Do odvolání
Odpovídající CPS	Certifikační prováděcí směrnice PostSignum QCA České Pošty, verze 1.25.

1.4 Zúčastněné strany a oblast použití

Česká pošta, s.p. ustavila hierarchii certifikačních autorit PostSignum QCA, jejímž kořenem je PostSignum Root QCA. Podřízené certifikační autority, kterým je vydáván certifikát podle této certifikační politiky, musí být řízeny a provozovány Českou poštou, s.p.

1.4.1 Poskytovatel certifikačních služeb

Poskytovatelem certifikačních služeb je Česká pošta, s.p.

1.4.2 PostSignum Root QCA

PostSignum Root QCA tvoří kořen hierarchie certifikačních autorit působících v rámci PostSignum QCA. Jejím úkolem je především vydávat a spravovat certifikáty certifikačních autorit působících v rámci České pošty.

1.4.3 Klienti PostSignum Root QCA

PostSignum Root QCA vydává kvalifikované systémové certifikáty ve smyslu zákona o elektronickém podpisu [ZoEP] těm certifikačním autoritám, jejichž certifikační politiky jsou v souladu s koncepcí a posláním PostSignum QCA České pošty. Certifikační politiky těchto autorit musí být schváleny komisí pro certifikační politiky ČP. Certifikačním autoritám, jejichž politiky nebyly komisí pro certifikační politiky ČP schváleny, nesmí být vydán certifikát podle této politiky.

1.5 Oblast použití

Kvalifikované systémové certifikáty vydané podle této certifikační politiky mohou být použity pouze pro ověření elektronického podpisu podřízené certifikační autority v hierarchii PostSignum QCA v souladu se zákonem o elektronickém podpisu [ZoEP].

1.5.1 Omezení použití certifikátu

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

1.6 Správa certifikační politiky

1.6.1 Správce dokumentu

Za správu této certifikační politiky a za její soulad s dokumentem Certifikační prováděcí směrnice odpovídá manažer PostSignum QCA.

1.6.2 Komise pro certifikační politiky České pošty

Komise pro certifikační politiky České pošty (PAA ČP) je orgán, který ustavuje, sleduje a udržuje certifikační politiky, jimiž se řídí činnost PostSignum QCA. Jedná se jak o politiky pro kořenovou certifikační autoritu (PostSignum Root QCA), tak o politiky pro podřízené certifikační autority.

1.6.3 Správa dokumentu

Tento dokument je vytvářen týmem pro tvorbu certifikačních politik ČP (Policy Creation Authority - PCA PostSignum QCA), který je dále zodpovědný za tvorbu certifikačních politik. PCA PostSignum QCA je dle potřeby ustavován Komisí pro certifikační politiky ČP, je jí řízen a kontrolován. PCA PostSignum QCA předává dokument ke schválení Komisi pro certifikační politiky.

Nové verze certifikačních politik a certifikační prováděcí směrnice vznikají podle potřeby, zejména však:

- při vzniku nového typu certifikátu,
- při takové změně PostSignum QCA (např. změně postupů), která ovlivní obsah těchto dokumentů,
- pokud při pravidelné kontrole okolního prostředí PostSignum QCA byly identifikovány požadavky na změny těchto dokumentů.

1.6.4 Změny v certifikační politice

Za iniciování změn v certifikační politice nebo inicializaci vytvoření nové certifikační politiky je odpovědný manažer PostSignum QCA. Ten předá požadavek týmu pro tvorbu certifikačních politik (PCA).

Veškeré změny v této certifikační politice podléhají schválení Komise pro certifikační politiky ČP (PAA ČP). PAA ČP přidělí nové verzi certifikační politiky číslo verze, které se promítne rovněž do identifikátoru politiky (OID).

Nová verze certifikační politiky bude zveřejněna na www serveru PostSignum QCA. PAA ČP rozhodne, zda je nutné zveřejnit informaci o nové verzi certifikační politiky též jinou formou, případně jak.

1.6.5 Platnost dokumentu

Platnost tohoto dokumentu je uvedena v kapitole 1.3.

1.6.6 Ukončení platnosti dokumentu

Platnost tohoto dokumentu je ukončena dnem ukončení platnosti posledního certifikátu vydaného podle této certifikační politiky.

1.7 Kontaktní informace

1.7.1 Poskytovatel certifikačních služeb

Poskytovatelem certifikačních služeb PostSignum Root QCA je

Česká pošta, s.p., IČ 47114983

se sídlem

Olšanská 38/9, 225 99 Praha 3

1.7.2 Provozní kontaktní údaje

S dotazy a požadavky spojenými s provozem PostSignum QCA, například s žádostmi o zneplatnění certifikátů, se obracejte na následující adresu:

Česká pošta, s.p.,

Manažer PostSignum QCA

Olšanská 38/9, 225 99 Praha 3

nebo prostřednictvím elektronické pošty na adrese

manager.postsignum@cpost.cz

1.7.3 Správce dokumentu

Za správu tohoto dokumentu odpovídá manažer PostSignum QCA. Kontaktní adresa manažera PostSignum QCA je

manager.postsignum@cpost.cz

1.7.4 Komise pro certifikační politiky České pošty

Komisi pro certifikační politiky ČP lze kontaktovat na adrese

paa.postsignum@cpost.cz

1.7.5 PostSignum Root QCA

www server certifikační autority PostSignum Root QCA má adresu

http://www.postsignum.cz

Adresářové služby certifikační autority PostSignum Root QCA jsou dostupné na adrese

ldap://qca.postsignum.cz

Certifikát PostSignum Root QCA je zveřejněn rovněž v Poštovním věstníku.

1.7.6 Kontaktní osoba

Kontaktní osobou pro PostSignum Root QCA je manažer PostSignum QCA. Adresa kontaktní osoby:

manager.postsignum@cpost.cz

1.7.7 Osoba odpovědná za soulad CPS s CP

Osobou odpovědnou za soulad certifikační prováděcí směrnice s touto politikou je manažer PostSignum QCA, jehož adresa je:

manager.postsignum@cpost.cz.

1.8 Použité zkratky a pojmy

QCA ČP - viz. PostSignum QCA

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

Držitel certifikátu – zákazník od okamžiku vydání certifikátu.

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

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

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

PostSignum QCA - Hierarchie certifikačních autorit, vydávajících kvalifikované certifikáty a kvalifikované systémové certifikáty ve smyslu zákona o elektronickém podpisu [ZoEP].

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

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

Obchodní místo – centrální regionální pracoviště odpovědné za uzavírání a evidenci smluv (typicky se jedná o pracoviště marketingu PTJ VT).

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

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

Správa žadatelů - aplikace QCA 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 Qualified CA například pro ověření digitálního podpisu nebo pro zajištění jiných bezpečnostních služeb. Jinak též označována jako Osoba spoléhající se na certifikát.

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

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

2. ZVEŘEJŇOVÁNÍ A UCHOVÁVÁNÍ INFORMACÍ

2.1 Uložení dat, jejich správa a zásady zveřejňování

Vydané certifikáty jsou uloženy v adresářovém serveru České pošty, s.p a v databázi certifikační autority.

Informace o vydaných certifikátech, stavu certifikátů a seznamech zneplatněných certifikátů jsou poskytovány prostřednictvím adresářových služeb a pomocí www rozhraní na www serveru České pošty, s.p.

Prostřednictvím adresářového serveru i www rozhraní jsou přístupné pouze ty certifikáty (a s nimi spojené informace), u nichž držitel certifikátu souhlasil se zveřejněním.

Prostřednictvím www serveru poskytovatele certifikačních služeb jsou dále poskytovány následující služby:

- vyhledání a stažení certifikátu PostSignum Root QCA,
- vyhledání a stažení certifikátu podřízených certifikačních autorit,
- zpřístupnění CRL PostSignum Root QCA,
- stažení certifikátu.

Přístup k těmto službám není nijak omezen.

2.2 Zveřejňování certifikátů a CRL

Certifikáty a CRL jsou přístupné na adresách

http://www.postsignum.cz/

ldap://qca.postsignum.cz

ldap://postsignum.ttc.cz

CRL je zveřejňován rovněž na adrese

http://postsignum.ttc.cz/crl/psrootqca.crl

2.3 Zveřejňování informací o certifikační autoritě

Každá certifikační autorita v hierarchii PostSignum QCA zveřejňuje své certifikační politiky na www serveru PostSignum QCA.

Zde jsou zveřejněny také certifikáty certifikačních autorit včetně PostSignum Root QCA, jejíž certifikát a otisk tohoto certifikátu jsou navíc zveřejněny v Poštovním věstníku.

2.4 Periodicita zveřejňování

Certifikáty vydané PostSignum Root QCA, u nichž byl vysloven souhlas se zveřejněním, jsou zveřejňovány elektronickou cestou nejpozději do 24 hodin od převzetí certifikátu držitelem (viz odstavec 4.3).

Certifikát vydaný podle této certifikační politiky bude zneplatněn nejpozději následující pracovní den po přijetí oprávněné žádosti o zneplatnění.

Seznamy zneplatněných certifikátů (CRL) jsou vydávány a zveřejňovány alespoň jednou za dvanáct měsíců. V případě zneplatnění certifikátu vydaného PostSignum Root QCA je CRL, na němž je tento certifikát uveden, zveřejněn do dvanácti hodin od zneplatnění certifikátu.

Nové certifikační politiky a revize stávajících politik jsou zveřejňovány na www serveru PostSignum QCA po schválení Komisí pro certifikační politiky ČP.

2.5 Řízení přístupu k informacím

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

Poskytovatel certifikačních služeb neumožňuje přístup k vydaným certifikátům, u kterých nebyl držitelem vysloven souhlas se zveřejněním. Přístup k vydaným certifikátům, u kterých byl držitelem vysloven souhlas se zveřejněním, je omezen na vyhledání těchto certifikátů podle zadaného kriteria.

Modifikace zveřejněných údajů je povolena pouze autorizované obsluze a procesům certifikační autority.

3. IDENTIFIKACE A AUTENTIZACE

3.1 Registrace žadatelů o certifikát

Certifikáty se vydávají pro certifikační autority, jejichž provozovatelem je Česká pošta. Oprávněným žadatelem o certifikát podřízené certifikační autority je manažer dané certifikační autority. Svou totožnost a své oprávnění dokládá podle vnitřních předpisů České pošty.

3.2 Registrace žádostí o zneplatnění certifikátů

Oprávněným žadatelem o zneplatnění certifikátu podřízené CA je manažer této CA. Svou totožnost a své oprávnění dokládá podle vnitřních předpisů České pošty a na základě uzavřené smlouvy o poskytování certifikačních služeb.

Certifikát podřízené certifikační autority může být zneplatněn i z vůle provozovatele PostSignum Root QCA. V takovém případě je oprávněným žadatelem o zneplatnění certifikátu podřízené autority manažer PostSignum QCA.

O zneplatnění certifikátu vydaného jako kvalifikovaný může, jakožto o předběžné opatření, požádat i orgán definovaný zákonem o elektronickém podpisu. Oprávněným žadatelem o zneplatnění kvalifikovaného certifikátu je v tomto případě zástupce tohoto orgánu.

3.3 Registrace žádostí o obnovu certifikátu

Obnova certifikátu probíhá stejně jako registrace první žádosti a vydání prvního certifikátu žadateli o certifikát.

3.4 Znakové sady a transkripce údajů

V certifikátech vydávaných PostSignum Root QCA jsou podporovány pouze následující znakové sady:

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

Veškeré údaje dokladované při registraci žádosti o certifikát podřízené CA se do žádostí o certifikáty a do certifikátů vydávaných PostSignum Root QCA přenášejí ve tvaru, ve kterém jsou uvedeny v předkládaných dokladech. Transkripce, jako například odstranění diakritiky, není možná.

3.5 Jednoznačnost jmen a postup v případě kolize

PostSignum Root QCA si vyhrazuje právo upravit označení držitele certifikátu (položka Subject v certifikátu) tak, aby byla zaručena jednoznačnost jména, tedy aby stejné rozlišovací jméno nebylo přiřazeno dvěma různým subjektům.

3.6 Pseudonym

Česká pošta nepodporuje pseudonym v položce Subjekt certifikátu podřízené certifikační autority.

4. PROVOZNÍ POŽADAVKY

4.1 Žádost o certifikát

Písemná žádost o vydání certifikátu podřízené certifikační autority se předkládá Komisi pro certifikační politiky ČP. Žádost musí obsahovat následující identifikační údaje certifikační autority, pro kterou má být vydán certifikát:

- jméno certifikační autority,
- provozovatel certifikační autority - upřesnění provozovatele v rámci České pošty,
- seznam dokumentů přiložených k této žádosti včetně označení verzí těchto dokumentů,
- vyjádření souhlasu případně nesouhlasu se zveřejněním certifikátu.

Žádost musí být podepsána zástupcem CA oprávněným k podání žádosti.

K žádosti musí být přiloženy tyto dokumenty:

- certifikační politiky certifikační autority, pro niž má být vydán certifikát,
- certifikační prováděcí směrnice,
- systémová bezpečnostní politika,

- plán zvládání krizových situací a plán obnovy.

Písemné žádosti a veškeré přiložené doklady jsou archivovány po dobu 10 let od ukončení platnosti certifikátu.

4.2 Vydání certifikátu

Komise pro certifikační politiky ČP na základě předložené žádosti rozhodne, zda bude pro danou certifikační autoritu vydán certifikát. Rozhodnutí je žadateli o certifikát sděleno do třiceti pracovních dní od podání žádosti.

Po schválení písemné žádosti předá zástupce podřízené certifikační autority manažerovi QCA elektronickou žádost o certifikát ve formátu PKCS#10, obsahující relevantní údaje se stejnými hodnotami, jako jsou uvedeny v předaných dokumentech. Spolu s elektronickou žádostí o certifikát předává zástupce podřízené CA manažerovi QCA druhou písemnou žádost obsahující následující údaje:

- jméno certifikační autority,

- provozovatel certifikační autority - upřesnění provozovatele v rámci České pošty,

- opis veřejného klíče certifikační autority,

- seznam dokumentů přiložených k této žádosti včetně označení verzí těchto dokumentů,

- vyjádření souhlasu případně nesouhlasu se zveřejněním certifikátu.

Všechny uvedené údaje musí souhlasit s údaji uvedenými ve schválené písemné žádosti o certifikát. Pokud údaje souhlasí, je do deseti pracovních dnů od okamžiku podání této žádosti vydán certifikát.

Certifikát se stává platným okamžikem vydání.

4.3 Převzetí certifikátu

Poskytovatel certifikačních služeb informuje žadatele o certifikát o vydání certifikátu nejpozději do jednoho pracovního dne od vydání certifikátu. Certifikát podřízené CA je žadateli o certifikát předán na disketě ve formátu DER spolu s certifikátem PostSignum Root QCA. Žadatel o certifikát nebo jeho zplnomocněný zástupce osobně přebírá certifikát a kontroluje, zda jsou údaje uvedené v certifikátu v pořádku. Pokud údaje souhlasí, žadatel přebírá certifikát a tento úkon stvrzuje svým podpisem pod protokolem o převzetí certifikátu. Pokud údaje nesouhlasí, poskytovatel certifikačních služeb musí do deseti pracovních dní vydat certifikát s opravenými údaji.

Podpisem protokolu o převzetí certifikátu držitel 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, které byly přeneseny ze žádosti o certifikát do certifikátu, jsou správné a úplné.

4.4 Obnova certifikátu

Obnova certifikátu vydaného podle této certifikační politiky není možná. Po ukončení platnosti stávajícího certifikátu požádá žadatel o vydání nového certifikátu; není nutné měnit subjekt certifikátu žadatele.

4.5 Použití klíče a certifikátu

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

4.6 Zneplatnění certifikátu

4.6.1 Důvody zneplatnění certifikátu

Certifikát může být zneplatněn z vůle držitele certifikátu, z vůle poskytovatele certifikačních služeb nebo na základně nařízení předběžného opatření orgánu definovaného zákonem o elektronickém podpisu.

4.6.2 Osoby oprávněné žádat o zneplatnění certifikátu

O zneplatnění certifikátu může požádat držitel certifikátu prostřednictvím manažera podřízené CA, manažer PostSignum Root QCA nebo zástupce orgánu definovaného zákonem o elektronickém podpisu.

4.6.3 Postup zneplatnění na žádost držitele certifikátu

Manažer podřízené certifikační autority žádá o zneplatnění certifikátu písemně. V žádosti o zneplatnění musí být uveden důvod zneplatnění.

4.6.4 Zneplatnění certifikátu z vůle PostSignum Root QCA

Poskytovatel certifikačních služeb může zneplatnit certifikát držitele, který provozuje podřízenou certifikační autoritu v rozporu s dokumenty, jež byly přiloženy k žádosti o certifikát. Důvodem zneplatnění může být rovněž nedodržování pravidel této certifikační politiky nebo podezření na kompromitaci klíče podřízené CA.

Manažer PostSignum QCA podává písemnou žádost o zneplatnění certifikátu podřízené CA, kterou předá některému z operátorů oprávněných provádět zneplatnění certifikátu. Po úspěšném zneplatnění certifikátu podřízené CA je vytvořen protokol o zneplatnění certifikátu, který je neprodleně zaslán manažerovi podřízené CA. Manažer podřízené CA je o zneplatnění certifikátu podřízené CA informován rovněž telefonicky nebo prostřednictvím elektronické pošty.

4.6.5 Zneplatnění certifikátu z vůle orgánu definovaného zákonem o elektronickém podpisu

O zneplatnění certifikátu vydaného jako kvalifikovaný systémový může, jakožto o předběžné opatření, požádat i orgán definovaný zákonem o elektronickém podpisu. Zástupce orgánu definovaného zákonem o elektronickém podpisu žádá o zneplatnění kvalifikovaného certifikátu písemně, v žádosti musí být uveden důvod zneplatnění certifikátu.

Po úspěšném zneplatnění certifikátu podřízené CA je vytvořen protokol o zneplatnění certifikátu, který je neprodleně zaslán manažerovi podřízené CA. Manažer podřízené CA je o zneplatnění certifikátu podřízené CA informován rovněž telefonicky nebo prostřednictvím elektronické pošty.

4.6.6 Časová prodleva od podání žádosti o zneplatnění

Certifikát vydaný podle této certifikační politiky bude zneplatněn nejpozději následující pracovní den po přijetí oprávněné žádosti o zneplatnění.

Do 12 hodin od zneplatnění certifikátu, vydaného podle této certifikační politiky, je zveřejněn CRL obsahující zneplatněný certifikát.

4.7 Informace o stavu certifikátu

Seznam zneplatněných certifikátů (CRL) PostSignum Root QCA je vydáván a zveřejňován alespoň každých 12 měsíců na třech místech:

- na www serveru České pošty, s.p.,
- v adresářových službách České pošty, s.p.,
- u nezávislého poskytovatele www a adresářových služeb.

Primárním zdrojem aktuálního CRL je www server České pošty, s.p.

PostSignum Root QCA neposkytuje informace o stavu certifikátu protokolem OCSP.

4.8 Konec platnosti certifikátu

Platnost certifikátu je ukončena v okamžiku jeho zneplatnění.

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. Pokud byl držitelem vysloven souhlas se zveřejněním certifikátu, je takový certifikát nadále přístupný na www serveru PostSignum QCA.

5. BEZPEČNOST FYZICKÁ, PROCEDURÁLNÍ A PERSONÁLNÍ

Fyzická, procedurální a personální bezpečnost PostSignum QCA se řídí platnými předpisy České pošty. Tato kapitola je podrobně rozpracována v Certifikační prováděcí směrnici.

5.1 Ukončení činnosti PostSignum Root QCA

Ukončení činnosti PostSignum Root QCA musí být písemně oznámeno všem držitelům platných certifikátů a rovněž zveřejněno na www serveru PostSignum uvedeném v kapitole 1.7.5. 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.

ČP prokazatelně zničí data pro vytváření elektronického podpisu PostSignum Root QCA, která sloužila pro podepisování kvalifikovaných certifikátů a seznamů zneplatněných certifikátů.

5.1.1 Podezření na kompromitaci soukromého klíče PostSignum Root QCA

V případě podezření na kompromitaci soukromého klíče PostSignum Root QCA budou písemně informováni všichni držitelé certifikátů o mimořádném ukončení činnosti, oznámení bude rovněž zveřejněno na www serveru PostSignum uvedeném v kapitole 1.7.5 a na všech kontaktních místech PostSignum QCA ČP. 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 elektronického podpisu PostSignum Root QCA, která sloužila pro podepisování kvalifikovaných certifikátů a seznamů zneplatněných certifikátů, u nichž existuje podezření na kompromitaci.

5.2 Ukončení činnosti kvalifikovaného poskytovatele certifikačních služeb

Činnost kvalifikovaného poskytovatele certifikačních služeb bude ukončena v souladu s §13 zákona o elektronickém podpisu [ZoEP].

6. TECHNICKÁ BEZPEČNOST

Česká pošta, jakožto poskytovatel certifikačních služeb, věnuje náležitou péči ochraně soukromých klíčů certifikačních autorit a komponent PKI v hierarchii PostSignum QCA. Tato kapitola je podrobně rozpracována v Certifikační prováděcí směrnici.

6.1 Ochrana klíčů autority

Soukromý klíč PostSignum Root QCA je generován a uschováván v zařízení, které splňuje požadavky standardu FIPS 140-1 Level 4. Použité algoritmy a jejich parametry odpovídají požadavkům zákona o elektronickém podpisu [ZoEP] v platném znění a navazujících předpisů. Délka klíče pro algoritmus RSA je 2048 bitů.

6.2 Ochrana klíčů držitelů certifikátů

Soukromé klíče žadatelů o certifikát musí být generovány a uschovávány v zařízení splňujícím alespoň požadavky FIPS 140-1 Level 3. Použité algoritmy a jejich parametry musí odpovídat požadavkům zákona o elektronickém podpisu [ZoEP] v platném znění a navazujících předpisů. Délka klíče pro algoritmus RSA musí být 2048 bitů.

7. PROFIL CERTIFIKÁTU, CRL A ŽÁDOSTI O CERTIFIKÁT

Tab. 2 Profil certifikátu podřízené CA

Version	3 (0x2)
Serial Number	*PostSignum Root QCA přiřazuje každému vydanému certifikátu jednoznačné číslo.*
SignatureAlgorithm	sha1WithRSAEncryption
Issuer	
Country	CZ
Organisation	Česká pošta, s.p. [IČ 47114983]
CN	PostSignum Root QCA
Validity	
Not Before	*Datum vydání - UTCTime*
Not After	*15 let od data vydání - UTCTime*
Subject	
Country	CZ

Organisation	Česká pošta, s.p. [IČ 47114983]
Locality	*Sídlo podřízené certifikační autority. Nepovinná položka*
OU	*Organizační jednotka, která provozuje CA. Nepovinná položka*
CN	*jméno certifikační autority*
Subject Public Key Info	
Algorithm	rsaEncryption
SubjectPublicKey	*veřejný klíč označující osoby*
Extensions	*rozšíření certifikátu podle tabulky 3*
Signature	*elektronická značka poskytovatele certifikačních služeb*

Položka Subject certifikátu jednoznačně identifikuje označující osobu, případně prostředek pro vytváření elektronických značek označující osoby.

Tab.3 Rozšíření v certifikátu

Název rozšiřující položky	Hodnota/příznak použití	Kritická ano/ne
Authority Key Identifier		ne
Key Identifier	*používá se*	
AuthorityCertIssuer	*používá se*	
AuthorityCertSerialNumber	*používá se*	
Subject Key Identifier	*používá se*	
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 byl vydan jako kvalifikovany systemovy certifikat ve smyslu zakona 227/2000 Sb. a navazujicich predpisu.	
CRL Distribution Points	URI: http://www.postsignum.cz/crl/psrootqca.crl URI: http://postsignum.ttc.cz/crl/psrootqca.crl URI: ldap://qca.postsignum.cz/cn=PostSignum Root QCA,o=Ceska posta s.p. [IC 47114983],c=CZ URI: ldap://postsignum.ttc.cz/cn=PostSignum Root QCA,o=Ceska posta s.p. [IC 47114983],c=CZ	ne
Basic Constraints	cA:TRUE PathLenConstraint:0	ne

Tab.4 Profil CRL

Version	2 (0x1)
Issuer	
Country	CZ
Organisation	Česká pošta, s.p. [IČ 47114983]
CN	PostSignum Root QCA
Validity	
This Update	*Datum vydání*

Next Update	*Datum vydání + 12 měsíců*
RevokedCertificates	*opakující se položka pro každý zneplatněný certifikát*
UserCertificate	*sériové číslo zneplatněného certifikátu*
RevocationDate	*datum a čas zneplatnění*
CrlEntryExtensions	*důvod zneplatnění certifikátu*
CrlExtensions	*rozšíření CRL podle tabulky 5*
SignatureAlgorithm	sha1WithRSAEncryption
Signature	*elektronická značka poskytovatele certifikačních služeb*

Tab.5 Rozšíření v CRL

Název rozšiřující položky	*Hodnota/příznak použití*	*Kritická ano/ne*
Rozšíření pro CRL		
Authority Key Identifier		ne
Key Identifier	*používá se*	
AuthorityCertIssuer	*používá se*	
AuthorityCertSerialNumber	*používá se*	
CRL Number	*PostSignum Qualified CA přiřadí každému CRL jednoznačné číslo.*	ne

7.1 Žádost o certifikát

Česká pošta přijímá elektronické žádosti o certifikát ve formátu PKCS#10, kódování DER a BASE64. Součástí elektronické žádosti o certifikát musí být veřejný klíč žadatele o certifikát a dále tyto položky:

Tab.6 Profil žádosti o certifikát

Položka	Obsah	Poznámka
Subject		
Country	CZ	
Organisation	Česká pošta, s.p. [IČ 47114983]	
Locality	*Sídlo podřízené certifikační autority*	Pokud má být v certifikátu uvedeno
OU	*Organizační jednotka, která provozuje CA*	Pokud má být v certifikátu uvedeno
CN	*Jméno certifikační autority*	

7.2 Certifikát PostSignum Root QCA

7.2.1 Profil samopodepsaného certifikátu

Tab.7 Profil certifikátu PostSignum Root QCA

Version	3 (0x2)
Serial Number	*PostSignum Root QCA přiřazuje každému vydanému certifikátu jednoznačné číslo.*
SignatureAlgorithm	sha1WithRSAEncryption
Issuer	
Country	CZ
Organisation	Česká pošta, s.p. [IČ 47114983]
CN	PostSignum Root QCA
Validity	
Not Before	*Datum vydání - UTCTime*
Not After	*25 let od data vydání - UTCTime*
Subject	
Country	CZ
Organisation	Česká pošta, s.p. [IČ 47114983]
CN	PostSignum Root QCA

Subject Public Key Info	
Algorithm	rsaEncryption
SubjectPublicKey	*veřejný klíč označující osoby*
Extensions	*rozšíření certifikátu podle tabulky 8*
Signature	*elektronická značka poskytovatele certifikačních služeb*

Tab.8 Rozšíření v certifikátu PostSignum Root QCA

Název rozšiřující položky	**Hodnota/příznak použití**	**Kritická ano/ne**
Authority Key Identifier		ne
Key Identifier	*používá se*	
AuthorityCertIssuer	*používá se*	
AuthorityCertSerialNumber	*používá se*	
Subject Key Identifier	*používá se*	
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 byl vydan jako kvalifikovany systemovy certifikat ve smyslu zakona 227/2000 Sb. a navazujicich predpisu.	
CRL Distribution Points	URI: http://www.postsignum.cz/crl/psrootqca.crl URI: http://postsignum.ttc.cz/crl/psrootqca.crl URI: ldap://qca.postsignum.cz/cn=PostSignum Root QCA,o=Ceska posta s.p. [IC 47114983],c=CZ URI: ldap://postsignum.ttc.cz/cn=PostSignum Root QCA,o=Ceska posta s.p. [IC 47114983],c=CZ	ne
Basic Constraints	cA:TRUE PathLenConstraint:1	ne

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

7.7.2 Výpis certifikátu

Výpis certifikátu PostSignum Root QCA bude zveřejněn jako příloha této certifikační politiky po jeho vytvoření.

8. HODNOCENÍ SHODY A SOULADU S PŘEDPISY

8.1 Audit

Činnost PostSignum QCA podléhá auditu. Audit PostSignum QCA provádí nejméně jednou čtvrtletně interní auditor, jednou ročně je provoz PostSignum QCA prověřen externím auditorem nezávislým na České poště, s.p.

8.2 Oblasti auditu

V rámci pravidelného interního auditu je hodnocen běžný provoz PostSignum QCA. Interní audity provádí Auditor PostSignum QCA.

Oblasti hodnocené v rámci pravidelných externích auditů jsou specifikovány v certifikační prováděcí směrnici.

8.3 Opatření v případě zjištění nedostatků

Výsledky auditu jsou předávány manažerovi PostSignum QCA, který zajistí nápravu zjištěných nedostatků.

8.4 Archivace záznamů

Záznamy o činnosti PostSignum QCA jsou archivovány po dobu deseti let.

8.4.1 Typy uchovávaných archivních záznamů

V PostSignum QCA se archivují tyto záznamy:

- programové vybavení a data, včetně vydaných certifikátů a CRL,
- veškerá papírová dokumentace související s registrací žádosti o certifikát a žádosti o zneplatnění certifikátu, včetně smluv,
- veškeré logy automaticky vytvářené komponentami informačního systému PostSignum QCA.

9. DALŠÍ OBCHODNÍ A PRÁVNÍ ZÁSADY

9.1 Poplatky za služby

Protože veškeré certifikační autority v rámci hierarchie PostSignum QCA provozuje Česká pošta, není cena za certifikáty vydané PostSignum Root QCA stanovena.

9.2 Finanční odpovědnost

9.2.1 Pojistné krytí

Česká pošta má sjednané pojištění odpovědnosti za škodu. Smlouva je uzavřena s následujícími pojišťovnami: Kooperativa, pojišťovna, a.s., Česká pojišťovna a.s. a Česká podnikatelská pojišťovna, a.s.

Pro všechny zaměstnance České pošty je sjednáno pojištění odpovědnosti za škodu způsobenou zaměstnavateli při výkonu povolání. Smlouva je uzavřena s Českou podnikatelskou pojišťovnou, a.s.

9.2.2 Aktiva ČP

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

K nahlédnutí je též na www serveru České pošty (www.cpost.cz).

9.3 Ochrana důvěrných informací

Certifikační autority, kterým byl vydán certifikát podle této certifikační politiky, jsou provozovány Českou poštou, stejně jako PostSignum Root QCA.

9.4 Ochrana osobních údajů

Česká pošta zajišťuje ochranu osobních údajů osob, k nimž získá přístup při poskytování certifikačních služeb. Zásady ochrany osobních údajů jsou obsaženy v této certifikační politice, všeobecných obchodních podmínkách ČP [VOP] a v Certifikační prováděcí směrnici [CPS] a vycházejí z příslušných ustanovení zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.

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

9.4.1 Zpřístupnění osobních údajů orgánům zmocněným ze zákona

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 PostSignum QCA poté, co orgány zmocněné ze zákona prokáží své zmocnění způsobem obvyklým v těchto případech.

9.5 Ochrana 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 webové stránky certifikační autority (www.postsignum.cz).

9.6 Záruky ČP

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

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

9.7 Omezení záruk

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

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

9.8 Odpovědnost

9.8.1 Odpovědnost ČP

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

b) 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.

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

9.8.2 Odpovědnost spoléhající se osoby

Odpovědnost spoléhající se osoby se řídí obecně závaznými právními předpisy.

9.9 Obecné zásady

9.9.1 Komunikační jazyk

Veškerá komunikace mezi žadatelem o certifikát a poskytovatelem certifikačních služeb musí probíhat v českém jazyce, pokud se obě strany nedohodnou jinak.

9.9.2 Použitelnost certifikátů

Certifikáty vydané podle této certifikační politiky mohou být použity pouze k ověření elektronických podpisů podřízené certifikační autority v hierarchii PostSignum QCA v souladu se zákonem o elektronickém podpisu [ZoEP].

9.9.3 Povinnosti

9.9.3.1 Povinnosti držitelů certifikátů

Držitelé certifikátů jsou povinni chránit soukromý klíč odpovídající veřejnému klíči v certifikátu. Klíč musí být chráněn zejména proti modifikaci, prozrazení nepovolaným osobám a neoprávněnému použití.

Soukromý klíč odpovídající veřejnému klíči v certifikátu vydaném podle této certifikační politiky nesmí být použit k jiným účelům než

- k podpisu certifikátů subjektů, které nejsou certifikačními autoritami,
- k podpisu seznamu zneplatněných certifikátů (Certificate Revocation List - CRL)

v souladu se zákonem o elektronickém podpisu [ZoEP].

Soukromý klíč nesmí být uschováván nechráněný. Zařízení, ve kterém je soukromý klíč uložen, musí minimálně splňovat požadavky kladené standardem FIPS 140-1 Level 3 nebo poskytovat obdobné záruky bezpečnosti. V případě prozrazení soukromého klíče musí držitel certifikátu o této skutečnosti bez prodlení informovat PostSignum Root QCA a požádat o revokaci certifikátu.

V žádosti o certifikát musí být uvedeny pouze pravdivé údaje. Držitel certifikátu je povinen zkontrolovat, zda údaje uvedené v certifikátu jsou správné a odpovídají údajům uvedeným v žádosti.

O případných nesrovnalostech musí bez prodlení informovat PostSignum Root QCA.

Držitel platného certifikátu je povinen neprodleně informovat PostSignum Root QCA

- o změnách údajů, které jsou uvedeny v certifikátu,
- o změnách, které mohou mít vliv na rozhodnutí PostSignum Root QCA vydat certifikát (viz odstavec 4.1).

Podle charakteru změn bude komisí pro certifikační politiky ČP rozhodnuto, zda bude certifikát podřízené certifikační autority zneplatněn, případně zda bude vydán certifikát nový.

9.9.3.2 Povinnosti poskytovatele certifikačních služeb

Poskytovatel certifikačních služeb má tyto povinnosti:

- věnovat náležitou péči všem činnostem spojeným s poskytováním certifikačních služeb; náležitá péče zahrnuje provoz v souladu
  - s provozní dokumentací,
  - s příslušnou certifikační politikou,
  - s platnou certifikační prováděcí směrnicí,
  - s platnými právními předpisy,
- ve sféře své působnosti vynucovat dodržování pravidel popsaných v certifikační prováděcí směrnici,
- zveřejňovat certifikační politiku, podle které vydává certifikáty, na www serveru PostSignum QCA, případně jinými vhodnými způsoby,
- zveřejnit samopodepsaný certifikát i otisk samopodepsaného certifikátu alespoň dvěma na sobě nezávislými způsoby,
- do 30 pracovních dnů posoudit žádost o certifikát, vydat rozhodnutí, zda bude certifikát vydán a o tomto rozhodnutí informovat žadatele o certifikát,
- vydat certifikát vyhovující standardu X.509 a splňující požadavky žadatele o certifikát,
- vydat certifikát obsahující věcně správné údaje na základě informací, které jsou certifikační autoritě k dispozici v době vydávání certifikátu, bez chyb způsobených obsluhou certifikační autority při zadávání údajů,
- informovat žadatele o certifikát o tom, že certifikát byl vydán, a předat vydaný certifikát žadateli,
- zveřejnit certifikát, u kterého byl vysloven souhlas se zveřejněním, do 24 hodin od převzetí certifikátu držitelem, způsobem popsaným v odstavci 2 této certifikační politiky,
- zneplatňovat certifikáty podle pravidel popsaných v této certifikační politice,

- informovat držitele certifikátu o tom, že jeho certifikát byl zneplatněn z vůle poskytovatele certifikačních služeb nebo z vůle orgánu definovaného zákonem o elektronickém podpisu,

- zveřejnit aktualizovaný seznam zneplatněných certifikátů do 12 hodin od zneplatnění certifikátu,

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

- provádět bezpečnostní audit v souladu s auditní a archivační politikou.

9.9.3.3 Povinnosti spoléhajících se stran a ostatních uživatelů

Uživatel certifikátu vydaného PostSignum Root QCA musí zejména:

- Získat certifikát PostSignum Root QCA z bezpečného zdroje (www server poskytovatele certifikačních služeb, www server orgánu definovaného zákonem o elektronickém podpisu) a ověřit otisk („fingerprint“) tohoto certifikátu.

- Před použitím certifikátu vydaného PostSignum Root QCA ověřit platnost certifikátu PostSignum Root QCA a následně i platnost vydaného certifikátu podřízené CA; kontrola se provádí na správnost podpisu vydávající autority a proti příslušnému aktuálnímu CRL.

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

10. LITERATURA

[ZoEP] Zákon 227/2000 o Sb. o elektronickém podpisu ve znění pozdějších předpisů

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

[CPS] Certifikační prováděcí směrnice PostSignum QCA, verze 1.25, vydaná dne 5.4.2005

[VOP] Všeobecné obchodní podmínky elektronických služeb České pošty, s.p.