Certifikační autorita

Příručka pro zákazníky – nepodnikající fyzické osoby

verze 2.0

druh dokumentu:	identifikace dokumentu:
Provozní dokument	**QCA P54**

Srpen 2010

Verze	Datum	Autor	Poznámka
1.0	14.1.2006	M.Šlancar	první verze
1.0.1	19.1.2006	M.Šlancar	opravena chyba v kapitole 4.1
1.0.3	23.9.2006	M.Šlancar	aktualizovány postupy a obrázky na základě změny webových stránek a zákaznických formulářů
1.0.4	18.8.2007	M.Šlancar	aktualizován seznam osobních dokladů v kapitole 6
2.0	6.9.2010	P. Huptich	Aktualizovány postupy na základě nových formulářů a webových stránek

Schváleno:

Verze	Schválil	
1.0	Manažer QCA	manager.postsignum@cpost.cz
1.0.1	Manažer QCA	manager.postsignum@cpost.cz
1.0.3	Manažer QCA	manager.postsignum@cpost.cz
1.0.4	Manažer QCA	manager.postsignum@cpost.cz
2.0	Manažer QCA	manager.postsignum@cpost.cz

1 Obsah

Tento dokument slouží jako obecně doporučený postup pro zákazníky certifikační autority PostSignum. Dílčí odchylky od toho postupu (stejně jako případné nejasnosti) doporučujeme konzultovat s konkrétním obchodním místem.

2 Definice používaných pojmů

Pro certifikační autoritu České pošty - **PostSignum** - budeme v textu používat zkratku **CA**

Pro kvalifikovanou certifikační autoritu České pošty - **PostSignum QCA** - budeme v textu používat zkratku **QCA**. Můžete se také setkat s označením „Kvalifikovaná certifikační autorita“.

Komerční certifikační autorita České pošty - **PostSignum VCA** - je sesterskou autoritou QCA. Pro komerční autoritu se používá poněkud netradičně zkratka **VCA**. Tato autorita je totiž interně označována jako „Veřejná certifikační autorita“.

Pro Českou poštu, s.p. budeme v textu používat zkratku **ČP**.

Pobočka České pošty se službou Czech POINT je pracoviště ČP, na němž se provádí vydávání a zneplatnění certifikátů. Také zde dochází k uzavření smlouvy

Zákazníkem je myšlena fyzická osoba (jednotlivec), podnikající fyzická osoba (OSVČ) či právnická osoba (organizace), která vstoupila do smluvního vztahu s ČP s tím, že s ní byla uzavřena smlouva o poskytování certifikačních služeb ČP.

Pod pojmem **žadatel** je myšlena osoba, která se dostaví na pobočku české pošty se službou Czech POINT za účelem vydání certifikátu. Buď se jedná přímo o fyzické osoby, nebo v případě organizací o zaměstnance.

Identifikátor klienta MPSV je jedinečné číslo každé osoby, které přiděluje Ministerstvo práce a sociálních věcí. Žadatel o certifikát může požádat, aby toto číslo bylo obsaženo v jeho certifikátu. Identifikátor klienta MPSV v certifikátu může být vyžadován při komunikaci se státní správou. Přiřazení identifikátoru je bezplatné.

MPSV je zkratka Ministerstva práce a sociálních věcí.

Elektronický podpis představují určitá data, která jsou svázána s danou zprávou. Elektronický podpis generuje určitá osoba a lze pomocí něj ověřit, že zprávu podepsala právě tato osoba a že zpráva nebyla pozměněna.

Elektronická značka je zjednodušeně řečeno elektronický podpis generovaný automaticky technickým zařízením. Vzhledem k tomuto faktu se na elektronickou značku vztahují jiné právní účinky, a proto se používá jiný termín.

Dvojice **soukromý klíč/veřejný klíč** tvoří základ pro provádění operací dešifrování/šifrování dat a generování/ověřování elektronického podpisu. Zatímco soukromý klíč musí zůstat pouze ve vlastnictví dané osoby, veřejný klíč této osoby může být dostupný komukoliv.

Elektronická žádost o certifikát je datová struktura (uložená v souboru), pomocí níž lze žádat o certifikát. V žádosti je uložen veřejný klíč, který se „přenese“ do vydaného certifikátu.

Certifikát představuje datovou strukturu, která je svázána s určitou osobou. Pomocí certifikátu lze tedy tuto osobu jednoznačně identifikovat. Pomocí certifikátu lze ověřit

elektronický podpis dané osoby. Součástí vydaného certifikátu jsou informace o držiteli certifikátu, doba platnosti, účel použití, veřejný klíč a případně další informace. Obsah certifikátu je podepsán vydávající certifikační autoritou, aby bylo možné prokázat, že byl touto autoritou skutečně vydán.

Kvalifikovaný certifikát je certifikát sloužící k ověření elektronického podpisu. Od „obyčejného“ certifikátu se liší tím, že jej vystavila kvalifikovaná certifikační autorita.

Kvalifikovaný systémový certifikát je certifikát sloužící k ověření elektronické značky. Opět jej vystavuje kvalifikovaná certifikační autorita.

Certifikační politika je dokument, který stanovuje účel použití certifikátů vydávaných pod touto politikou. Dále definuje podmínky vydání certifikátu, revokace (zneplatnění) certifikátu, atd.

Zneplatnění certifikátu je proces, kdy je předčasně ukončena platnost certifikátu. Certifikát se musí zneplatnit, pokud jej nelze dále používat (např. z důvodu prozrazení, ale také havárie počítače apod.). Po zneplatnění se certifikát ocitá na seznamu zneplatněných certifikátů. Místo zneplatnění se také používá termín **revokace**.

Seznam zneplatněných certifikátů je datová struktura (uložená v souboru) obsahující seznam certifikátů, které byly zneplatněny. Tento seznam je veřejně dostupný, takže každý si může ověřit, jestli jeho certifikát (nebo např. certifikát komunikujícího partnera) je stále platný. Běžně se také používá anglický termín **certificate revocation list**, a především z něj odvozená zkratka **CRL**.

3 Úvod

3.1 Úvodní slovo

Děkujeme za váš zájem o služby certifikační autority České pošty, **PostSignum**. Cílem tohoto dokumentu je podat vám v přehledné formě veškeré informace, potřebné pro úspěšné vystavení certifikátu pro vaši osobu.

Certifikační autorita **PostSignum** byla od počátku připravována na poskytování služeb dvěma velmi odlišným skupinám zákazníků – organizacím a nepodnikajícím fyzickým osobám bez IČ.

V následujících kapitolách budou popsány postupy týkající se pouze nepodnikajících fyzických osob.

3.2 Stručně o uzavření smlouvy a vydání certifikátu

Fyzická osoba uzavře s Českou poštou smlouvu o poskytování certifikačních služeb tak, jak je v obchodním styku obvyklé.

Navržené postupy předpokládají okamžité vydání certifikátu po uzavření smlouvy. Nepodnikající fyzické osoby jsou kompletně odbavovány na pobočkách České pošty se službou Czech POINT.

V následujících kapitolách si detailněji popíšeme celý proces od přípravy objednávky a zákaznického formuláře přes uzavření smlouvy až po finální vydání certifikátu žadateli.

3.3 Zdroje informací o QCA/VCA

Otázky zákazníků týkající se postupů uzavření smlouvy, vydání a zneplatnění certifikátu zodpoví kterékoliv obchodní místo. S odbornějšími dotazy se obraťte na uživatelskou podporu. Většinu informací o CA naleznete také na webových stránkách na adrese http://www.postsignum.cz. Dále v textu se na tyto stránky budeme často odkazovat.

4 Než dojde k uzavření smlouvy...

4.1 Mám požádat o kvalifikovaný nebo komerční certifikát?

Kvalifikované certifikáty lze použít při komunikaci s orgány státní správy. Jejich nevýhodou je, že mohou být použity jen za účelem podepisování dat, zatímco komerční certifikáty mohou být použity i pro jejich zašifrování.

Výhodou komerčních certifikátů je, že mohou být použity nejen za účelem podepisování dat, ale také pro jejich zašifrování. Jejich nevýhodou je, že nemusí být akceptovány při komunikaci se státní správou.

Pokud tedy budete převážně komunikovat s úřady státní správy, bude pro vás patrně výhodnější zřízení kvalifikovaného certifikátu.
Pokud však chcete používat certifikáty pro zajištění šifrování dat, nevyhnete se pořízení komerčního certifikátu.

4.2 Mám certifikační služby využívat jako zástupce/zaměstnanec organizace, OSVČ či nepodnikající fyzická osoba?

Pokud bude vydaný certifikát sloužit k zajištění pracovních povinností vůči vašemu zaměstnavateli, budete vůči CA vystupovat jako zaměstnanec organizace. Stáhněte si správnou verzi tohoto dokumentu.

Pokud hodláte komunikovat se svými partnery (např. úřady státní správy) jako podnikající fyzická osoba, budete vůči CA vystupovat právě jako podnikající fyzická osoba (OSVČ). Stáhněte si správnou verzi tohoto dokumentu.

Pokud hodláte vydaný certifikát využívat pro své soukromé účely, budete vůči CA vystupovat jako nepodnikající fyzická osoba.

4.3 Jaké certifikáty vydávané QCA/VCA budu vlastně potřebovat?

Každá certifikační autorita nabízí obecně poměrně specializované služby. Zákazník by se měl předem rozhodnout, jaký typ certifikátu bude potřebovat. Příslušné informace o vydávaných certifikátech jsou uvedeny v certifikačních politikách - ty naleznete na webových stránkách www.postsignum.cz. V této kapitole se pokusíme vyjmenovat ty nejdůležitější body, které by

vám měly pomoci při výběru správného typu certifikátu pro vás. Dále uvedeme důležité informace související s vydáváním certifikátů.

- Certifikáty v CA jsou vydávány vždy na základě elektronických žádostí o certifikát. Žádost o certifikát by měla být schopna vygenerovat vaše aplikace spolu s klíčovým párem. Na webových stránkách CA je možné vygenerovat klíčový pár spolu s elektronickou žádostí o certifikát; klíčový pár s certifikátem pak stačí importovat do vaší aplikace.
- Fyzickým osobám mohou být vystaveny certifikáty podle těchto politik:

  Kvalifikované osobní certifikáty
  Komerční osobní certifikáty
  Kvalifikované systémové certifikáty
  Komerční serverové certifikáty
  Komerční šifrovací certifikáty

  Osobní certifikáty kvalifikované i komerční a jsou určeny pro osoby. Certifikáty vydané podle ostatních politik jsou určeny pro technická zařízení (např. aplikace na serverech).
- Kvalifikované osobní certifikáty použijete zejména pro komunikaci se státní správou. Pokud chcete komunikovat s úřady státní správy, chtějte, aby bylo v certifikátu obsaženo číslo „Identifikátor klienta MPSV“.
- O Kvalifikované systémové certifikáty budou žádat nejčastěji právě orgány státní správy, které hodlají provozovat tzv. elektronické podatelny. Fyzické osoby nebudou v drtivé většině případů tyto certifikáty potřebovat.
- Podle zákona nemohou být certifikáty vydávané QCA využívány pro šifrování dat.
- Pro šifrování dat jsou určeny certifikáty vydávané autoritou **PostSignum VCA** – komerční certifikáty..
- Komerční **c**ertifikáty nejsou uznávány při komunikaci s úřady státní správy. Pro komunikaci se státní správou použijte kvalifikované certifikáty.

4.4 Na jakém pracovišti mohu vyřídit potřebné náležitosti?

Nepodnikající fyzické osoby vyřizují veškeré náležitosti na pobočce České pošty se službou Czech POINT.

4.5 Mám si nechat přidělit Identifikátor klienta MPSV?

Identifikátor klienta MPSV je číslo, přidělované Ministerstvem práce a sociálních věcí (MPSV), které vás jednoznačně identifikuje jako osobu. Jedná se vlastně o obdobu rodného čísla s tím rozdílem, že z Identifikátoru klienta MPSV nelze vyčíst datum narození a pohlaví.

Identifikátor klienta MPSV může být vyžadován při komunikaci s některými úřady státní správy. Proto spíše doporučujeme zažádat si o jeho přidělení a uložení do vydávaných certifikátů. Přidělení Identifikátoru MPSV je zdarma.

4.6 Mám povolit zveřejnění certifikátu?

Zveřejnění či nezveřejnění certifikátu se nastavuje v údajích pro vydání certifikátu (zákaznickém formuláři).

Zveřejnění certifikátu znamená, že certifikát bude přístupný všem uživatelům, kteří si jej pak mohou stáhnout z webových stránek nebo adresářových služeb PostSignum CA.

Jelikož je certifikát ze své podstaty veřejná datová entita, zakažte jeho zveřejnění skutečně jen v případě, že k tomu máte vážný důvod.

5 Příprava na uzavření smlouvy

Uzavření smlouvy spočívá přípravě formuláře smlouvy zákazníkem a jejím potvrzení na pracovišti České pošty. Fyzická osoba dále České poště předává vyplněné údaje pro vydání certifikátu (zákaznický formulář). Ihned po uzavření smlouvy může být zákazníkovi vystaven certifikát.

5.1 Získání formulářů

Zákazník si stáhne z webových stránek CA formulář smlouvy a údaje pro vydání certifikátu (zákaznický formulář). Dokumenty mu také může zaslat obchodní místo.

5.2 Vyplnění objednávky

Formulář objednávky vyplňte podle těchto pokynů:

- V bodu **1** doplňte sekci **Zákazník** zadejte vaše jméno a adresu bydliště.
- V bodu **2** zaškrtněte, zda chcete uzavřít smlouvu na dobu určitou nebo neurčitou. Běžně se smlouva uzavírá na dobu neurčitou.
- V bodu **4** zvolte:
    - zda hodláte udělit souhlas s využíváním vašich osobních údajů za účelem marketingu a propagace produktů a služeb ČP
    - možnost zasílání upozornění na končící platnost certifikátu
    - přidělení identifikátoru klienta MPSV (IK MPSV)
- Do bodu **6** doplňte vaše údaje, místo a datum.

Vyplněný formulář smlouvy se vytiskne ve dvou exemplářích. smlouvu ještě nepodepisujte.

5.3 Vyplnění údajů pro vydání certifikátu (zákaznického formuláře)

V údajích pro vydání certifikátu (zákaznickém formuláři) si určujete, jaké certifikáty vám budou vydány.

- V bodě **1** doplňte své osobní údaje.
- V bodě **2** doplňte údaje o osobním certifikátu. Označte zda má být vydaný certifikát zveřejněn a přidělení identifikátoru IK MPSV do kvalifikovaného osobního certifikátu.
- V bodě **3** doplňte údaje o ostatních certifikátech. Označte zda má být vydaný certifikát zveřejněn

Pokud jméno certifikátu obsahuje tzv. doménové jméno (např. **cpost.cz** nebo **mojedomena.com**), musíte připojit k zákaznickému formuláři prohlášení vlastníka domény, v němž stvrzujete, že vlastníte danou doménu. Formulář lze stáhnout z webových stránek CA. (Předpokládáme však, že fyzické osoby většinou nebudou požadovat vydání systémových certifikátů s doménovými jmény.)

5.3.1 Změna údajů pro vydání certifikátu

- Doplňte „Číslo smlouvy“. Tento údaj naleznete v uzavřené smlouvě.
- V bodě **1** doplňte své osobní údaje.
- Pokud je vyžadována změna osobního certifikátu v bodě **3** doplňte původní a nové údaje o certifikátu. Označte zda má být vydaný certifikát zveřejněn a přidělení identifikátoru IK MPSV do kvalifikovaného osobního certifikátu.
- Pokud je vyžadována změna ostatních certifikátů v bodě **4** doplňte původní a nové údaje o certifikátu. Označte zda má být vydaný certifikát zveřejněn.

Pokud má zákazník kvalifikovaný nebo komerční osobní certifikát vydaný certifikační autoritou České pošty PostSignum, nemusí se dostavit osobně, ale může tento formulář včetně příloh poslat elektronicky podepsaným e-mailem na obchodní místo certifikační autority České pošty. Seznam obchodních míst, včetně kontaktů, je na webových stránkách www.postsignum.cz.

Pokud dochází ke změně jména certifikátu a jméno po změně obsahuje tzv. doménové jméno (např. **cpost.cz** nebo **mojefirma.com**), musí pověřená osoba připojit k příloze seznamu žadatelů prohlášení vlastníka domény, v němž stvrzuje, že vlastní danou doménu. Formulář lze stáhnout z webových stránek CA.

5.4 Vygenerování klíčů a elektronické žádosti o certifikát

Pokud si chcete po uzavření smlouvy nechat ihned vydat certifikát, musíte si na svém počítači vygenerovat klíčový pár a elektronickou žádost o certifikát. Pro tyto účely jsou na webových stránkách CA nabízeny příslušné nástroje.

6 Uzavření smlouvy a vydání certifikátu

Dostavíte se na pobočku České pošty se službou Czech POINT s:

- Vyplněným formulářem smlouvy (dvojí vyhotovení),
- Údaji pro vydání certifikátu (zákaznický formulář),
- elektronickou žádostí o certifikát,
- **dvěma** osobními doklady (občanský průkaz, cestovní pas, řidičský průkaz, průkaz ZTP nebo rodný list – povinně musí být vždy předložen první nebo druhý uvedený doklad).

Před operátorem podepíšete oba exempláře smlouvy.

Operátor provede zavedení do systému CA. Poté se může přistoupit k vydání certifikátu.

6.1 Vydání certifikátu

Vytiskne se písemná žádost o certifikát, kterou svým podpisem schválíte.

Na žádosti se uvádí tzv. heslo pro zneplatnění, které souvisí s procesem zneplatnění certifikátu (viz kapitola 6.33). Toto heslo určujete vy, nebo je možné jej nechat vygenerovat automaticky. Není nutné si je pamatovat, protože bude uvedeno v protokolu o vydání certifikátu. Heslo by se nemělo shodovat s jinými hesly, která běžně používáte.

Vydaný certifikát lze přijmout:

- osobně podepsáním protokolu o vydání certifikátu. V tomto případě je certifikát uložen na přenosné médium zákazníka.
- potvrzením přijetí přes www stránky PostSignum na základě došlého mailu

Máte také právo vydaný certifikát odmítnout.
Pozor! V případě odmítnutí vydaného certifikátu nemůže být okamžitě vydán nový certifikát. Musíte si vygenerovat nový klíčový pár a žádost o certifikát a navštívit pobočku České pošty znovu..

6.2 Instalace vydaného certifikátu

Certifikát se nainstaluje do aplikace, v níž byly vygenerovány klíče. Pokud tato aplikace slouží pouze pro generování klíčů, provede se export do souboru a následné natažení do cílové aplikace.

Spolu s vydaným certifikátem je potřeba nainstalovat do cílové aplikace také certifikáty certifikačních autorit PostSignum CA. Naleznete je na webových stránkách PostSignum CA.

Postupy instalace vydaného certifikátu a certifikátů certifikačních autorit lze stáhnout z webových stránek CA.

6.3 Zneplatnění certifikátu

Může dojít k situaci, kdy již nemůžete používat své klíče a vystavený certifikát; např. z důvodu prozrazení soukromého klíče (tj. odcizení počítače apod.), ale také např. kvůli havárii počítače. V takovém případě musíte požádat o zneplatnění svého certifikátu, který odpovídá prozrazenému (ztracenému) soukromému klíči.

Postupy zneplatnění certifikátu jsou uvedeny na www stránkách PostSignum www.postsignum.cz

6.4 Doručení dalších údajů pro vydání certifikátu (zákaznických formulářů)

Vyplněný zákaznický formulář(e) doručíte osobně na pobočku České pošty se službou Czech POINT osobně a podepíšete se před pracovníkem ČP. Pokud má zákazník kvalifikovaný nebo komerční osobní certifikát vydaný certifikační autoritou České pošty PostSignum, nemusí se dostavit osobně, ale může tento formulář včetně příloh poslat elektronicky podepsaným e-mailem na obchodní místo certifikační autority České pošty. Seznam obchodních míst, včetně kontaktů, je na webových stránkách www.postsignum.cz.

Operátor zanese údaje do systému CA. Poté může dojít k vydání nového certifikátu nebo certifikátu se změněnými údaji.

6.5 Změna uzavřené smlouvy s Českou poštou

V případě změny vašich osobních údajů nebo jiných ustanovení ve smlouvě je uzavřen dodatek ke smlouvě. Dodatek ke smlouvě lze stáhnout ze stránek CA www.postsignum.cz

7 Ostatní

7.1 Fakturace

Ceník služeb CA je k dispozici na webových stránkách CA.

Vydaný certifikát je zaplacen v hotovosti na pobočce České pošty se službou Czech POINT.

7.2 Platnost certifikátu a jeho obnova

Platnost certifikátu je jeden rok. Poté je nutné požádat o nový certifikát.

Pokud nedošlo ke změně vašich osobních údajů nebo údajů v certifikátu, lze následný certifikát vystavit:

- osobní návštěvou pobočky České pošty se službou Czech POINT
- pomocí www aplikace
- pomocí elektronicky podepsaného e-mailu odeslaného na podatelnu postsignum

Informace o možnosti obnovy certifikátu jsou uvedeny v e-mailové zprávě, která je odesílána před koncem platnosti certifikátu.

Pokud došlo ke změnám, doručíte na pobočku České pošty se službou Czech POINT změnu údajů pro vydání certifikátu. Budou provedeny příslušné změny v systému CA a informuje vás o provedení změn. Poté se můžete dostavit na pobočku České pošty se službou Zzech POINT nechat si vydat nový certifikát.

Obnova certifikátu je opět zpoplatněna. Cena certifikátu je stanovena podle aktuálně platného ceníku. Za certifikát vydaný na pobočce platíte v hotovosti, za vydání následného certifikátu platíte předem poukázáním příslušné částky na účet České pošty, který je vám zaslán e-mailem.