



Kvalifikovaná certifikační autorita

Příručka pro zákazníky – právnické osoby

verze 1.0.4

Provozní dokumentace

Březen 2007

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
1.0.2	19.2.2006	M.Šlancar	zrušen požadavek na přinesení prvního seznamu žadatelů osobně oprávněnou osobou
1.0.3	23.9.2006	M.Šlancar	aktualizovány postupy a obrázky na základě změny webových stránek a zákaznických formulářů
1.0.4	24.3.2007	M.Šlancar	oprávněná osoba může podat žádost o zneplatnění certifikátu také osobně na kontaktním místě

Schváleno:

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

1 Obsah

1 Obsah	3
2 Definice používaných pojmů	5
3 Úvod	7
3.1 Úvodní slovo.....	7
3.2 Stručně o uzavření smlouvy a vydání certifikátu.....	7
3.3 Zdroje informací o QCA.....	7
4 Než dojde k uzavření smlouvy	7
4.1 Mám požádat o kvalifikovaný nebo komerční certifikát?.....	7
4.2 Mám certifikační služby využívat jako zástupce/zaměstnanec organizace, OSVČ či nepodnikající fyzická osoba?.....	8
4.3 Jaké certifikáty vydávané QCA budu vlastně potřebovat?.....	8
4.4 Na jakém pracovišti mohu vyřídit potřebné náležitosti?.....	9
4.5 Mám si nechat přidělit Identifikátor klienta MPSV?.....	9
4.6 Mám povolit zveřejnění certifikátu?.....	10
5 Uzavření smlouvy	10
5.1 Získání formulářů.....	10
5.2 Vyplnění objednávky.....	10
5.3 Doručení objednávky na obchodní/kontaktní místo.....	11
5.3.1 Doručení poštou.....	11
5.3.2 Doručení osobní návštěvou oprávněné osoby zákazníka.....	11
5.4 Akceptace objednávky ze strany ČP.....	12
5.4.1 V případě doručení objednávky poštou.....	12
5.4.2 V případě doručení objednávky osobně oprávněnou osobou zákazníka.....	12
5.5 Vyplnění seznamů žadatelů.....	12
5.5.1 Úvodní list seznamu žadatelů.....	12
5.5.2 Příloha seznamu žadatelů Certifikáty pro ověření el. podpisu zaměstnance.....	12
5.5.3 Příloha seznamu žadatelů Certifikáty pro ověření el. značky organizace.....	13
5.5.4 Změnová příloha seznamu žadatelů Certifikáty pro ověření el. podpisu zaměstnance.....	14
5.5.5 Změnová příloha seznamu žadatelů Certifikáty pro ověření el. značky organizace.....	14
5.6 Doručení prvního seznamu žadatelů na obchodní nebo kontaktní místo.....	15
5.7 Doručení dalších seznamů žadatelů.....	15
5.8 Změna uzavřené smlouvy s Českou poštou.....	16
6 Vydání certifikátů žadatelům	16
6.1 Vygenerování klíčů a elektronické žádosti o certifikát.....	16
6.2 Vydání certifikátu zaměstnanci organizace.....	16
6.3 Instalace vydaného certifikátu.....	16
6.4 Zneplatnění certifikátu.....	17

7 Ostatní.....	18
7.1 Fakturace.....	18
7.2 Platnost certifikátu a jeho obnova.....	18
8 Názorný příklad.....	19
8.1 Informace o fiktivní firmě.....	19
8.2 Uzavření smlouvy o poskytování certifikačních služeb.....	19
8.2.1 Příprava objednávky.....	19
8.3 Příprava seznamů žadatelů.....	23
8.3.1 Vyplnění úvodního listu seznamu žadatelů.....	23
8.3.2 Vyplnění přílohy seznamu žadatelů Certifikáty pro ověření elektronického podpisu zaměstnance.....	24
8.3.3 Vyplnění přílohy seznamu žadatelů pro politiku Certifikáty pro ověření elektronické značky organizace.....	27
8.4 Doručení objednávky a seznamu žadatelů na obchodní místo.....	28
8.5 Vydání certifikátů žadatelům.....	29
8.5.1 Vygenerování elektronických žádostí o certifikát.....	29
8.5.2 Vydání certifikátů na kontaktním místě.....	30
8.5.3 Instalace vydaného certifikátu.....	30
8.6 Dodání dalších seznamů žadatelů.....	30

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

2 Definice používaných pojmů

Protože dále v textu budeme používat větší množství termínů, vysvětlíme nejprve jejich význam. Jednotlivé termíny jsme se snažili vysvětlit tak, aby byly srozumitelné pro laickou veřejnost.

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**.

Obchodní místo je pracoviště ČP, na němž dochází k uzavření smlouvy mezi zákazníkem (právnickou osobou) a ČP. Toto pracoviště také provádí zavedení zákazníků a žadatelů do systému QCA, které je nutné provést před samotným vydáváním certifikátů. Obsluhu tohoto pracoviště budeme označovat termínem **operátor obchodního místa (operátor OM)**.

Kontaktní místo je pracoviště ČP, na němž se provádí vydávání a zneplatnění certifikátů. Také zde může dojít k uzavření smlouvy (především s fyzickými osobami, OSVČ a malými organizacemi). Pro obsluhu kontaktního místa se používá termín **operátor registrační authority**, nebo také **operátor RA**.

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.

Statutárním zástupcem organizace je myšlena osoba, která byla pověřena jednat za danou organizaci. Tato osoba je uvedena např. v obchodním rejstříku nebo jiném registru. Statutárním zástupcem je tedy ředitel organizace (případně generální ředitel), starosta obce, předseda sdružení apod. Z hlediska QCA podepisuje statutární zástupce objednávku certifikačních služeb.

Oprávněná osoba je zástupce organizace (jeden i více), který pro QCA definuje, kteří zaměstnanci mohou žádat o jaké certifikáty. Oprávněnou osobou může být statutární zástupce, především u organizací se složitější organizační strukturou je však vhodnější jmenovat jinou osobu, např. vedoucí personálních oddělení jednotlivých organizačních jednotek.

Pod pojmem **žadatel** je myšlena osoba, která se dostaví na kontaktní místo za účelem vydání certifikátu. Buď se jedná přímo o fyzické osoby, nebo v případě organizací o zaměstnance. Žadatelem může být pochopitelně také statutární zástupce a oprávněná osoba zákazníka.

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 „přenes“ 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 kvalifikované certifikační autority České pošty, **PostSignum QCA**. Cílem tohoto dokumentu je podat vám v přehledné formě veškeré informace, potřebné pro úspěšné vystavení certifikátu pro vaši osobu nebo zaměstnance vaší organizace.

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

V tomto dokumentu jsou uvedeny postupy, které se týkají pouze organizací.

3.2 Stručně o uzavření smlouvy a vydání certifikátu

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

V objednávce certifikačních služeb se uvedou oprávněné osoby. Po uzavření smlouvy dodají oprávněné osoby obchodnímu místu seznamy žadatelů, kteří jsou následně zavedeni do systému QCA. Tímto okamžikem se mohou jednotliví žadatelé dostavit na kontaktní místa a nechat si vydat certifikát. Dochází zde tedy k určité prodlevě mezi uzavřením smlouvy a vydáním certifikátu. Takto nastavené postupy ale na druhou stranu zabraňují tomu, aby se každou jednotlivou žádostí o certifikát musel zabývat statutární zástupce zákazníka. Také žadatelé předkládají při vydávání certifikátu minimum vyžadovaných podkladů.

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

Poznámka:

Organizace po dobu platnosti smlouvy komunikují s tím obchodním místem, s nímž uzavřely smlouvu. Pokud došlo k uzavření smlouvy na kontaktním místě, komunikují organizace s obchodním místem, které je nadřizeno tomuto kontaktnímu místu.

3.3 Zdroje informací o QCA

Otázky zákazníků týkající se postupů uzavření smlouvy, vydání a zneplatnění certifikátu zodpoví kterékoliv kontaktní nebo obchodní místo. S odbornějšími dotazy se obraťte na uživatelskou podporu.

Většinu informací o QCA naleznete také na webových stránkách na adrese <http://qca.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.

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. V tomto případě si stáhněte správnou příručku pro zákazníky z webových stránek PostSignum VCA.

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 QCA vystupovat jako zaměstnanec organizace.

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

Pokud hodláte vydaný certifikát využívat pro své soukromé účely, budete vůči QCA vystupovat jako nepodnikající fyzická osoba. Stáhněte si správnou verzi tohoto dokumentu.

4.3 Jaké certifikáty vydávané QCA 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 QCA. 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 QCA 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 QCA je možné vygenerovat klíčový pár spolu s elektronickou žádostí o certifikát; klíčový pár s certifikátem pak stačí importovat do vaší aplikace.
- Pro organizace jsou připraveny politiky:
Certifikáty pro ověření elektronického podpisu zaměstnance,
Certifikáty organizace pro ověření elektronické značky.

Certifikáty podle první politiky jsou kvalifikované certifikáty a jsou určeny pro osoby. Certifikáty podle druhé politiky jsou kvalifikované systémové certifikáty a jsou určeny pro technická zařízení (aplikace na serverech).

- Certifikáty pro ověření elektronického podpisu použijete zejména pro komunikaci se státní správou. Především pokud chcete komunikovat s Ministerstvem práce a sociálních věcí, chtějte, aby bylo v certifikátu obsaženo číslo „Identifikátor klienta MPSV“. Uvedení tohoto čísla v certifikátu mohou v budoucnu požadovat další orgány státní správy.

- O certifikáty pro ověření elektronické značky budou žádat nejčastěji právě orgány státní správy, které hodlají provozovat tzv. elektronické podatelny.
- Podle zákona nemohou být certifikáty vydávané QCA využívány pro šifrování dat. V tom případě se spíše poohlédněte po komerčních certifikátech vydávaných sesterskou autoritou **PostSignum VCA**.
- Certifikáty vydávané organizacím obsahují údaje „IČO a jméno organizace“ a jméno zaměstnance (resp. jméno označující osoby), volitelně také údaje „jméno organizační jednotky“, „e-mailová adresa“ a „funkce zaměstnance v organizaci“.
- Přestože hovoříme o e-mailové adrese jako nepovinném údaji, rozhodně si nechte vydat certifikát s uvedenou e-mailovou adresou. Certifikát bez (správné) e-mailové adresy nelze použít pro odeslání podepsaných e-mailových zpráv. E-mailová adresa v kvalifikovaných certifikátech pro zaměstnance je **povinná**.

4.4 Na jakém pracovišti mohu vyřídit potřebné náležitosti?

Následující tabulka uvádí seznam činností a pracoviště, na kterých lze tyto činnosti vyřídit. Uvedené činnosti jsou vysvětlovány dále v textu

Činnost	Obchodní místo	Kontaktní místo
Uzavření smlouvy	ano	ano
Vložení základních informací o zákazníkovi do systému QCA	ano	ano
Vložení údajů ze seznamů žadatelů do systému QCA	ano	ano*
Vložení údajů z dalších seznamů žadatelů do systému QCA	ano	ne
Změny ve smlouvě / seznamech žadatelů	ano	ne
Vydání certifikátu	ne	ano
Zneplatnění certifikátu	ne	ano

* Platí pouze během tzv. zrychleného zavedení zákazníka do systému QCA na kontaktním místě:

- oprávněná osoba doručí osobně na kontaktní místo objednávku a zároveň seznamy žadatelů
- seznamy žadatelů mohou obsahovat pouze přílohy pro vydání certifikátů pro ověření elektronického podpisu zaměstnance bez vyplněného údaje certifikátu „OU (organizační jednotka)“
- po zavedení údajů do systému může proběhnout vydání certifikátu oprávněné osobě (je-li uvedena na seznamu žadatelů jako žadatel)

Toto omezení platí pouze pro první předání seznamů žadatelů. V dalších seznamech žadatelů již lze žádat o certifikáty pro ověření elektronické značky a certifikáty obsahující organizační jednotky.

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 na seznamu žadatelů.

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

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

5 Uzavření smlouvy

Postup uzavírání smlouvy s organizací počítá, že se jedná spíše o organizaci se složitější organizační strukturou. U „menších“ organizací mohou být některé body postupu zjednodušeny (určování oprávněných osob, uzavření smlouvy, odevzdání seznamů žadatelů a vydání certifikátu při jedné návštěvě kontaktního místa).

Uzavření smlouvy spočívá v přípravě objednávky zákazníkem, která se po akceptaci na straně ČP stává smlouvou o poskytování certifikačních služeb. Oprávněná osoba zákazníka dále doručí připravený seznam žadatelů, který může předat spolu s objednávkou nebo samostatně po uzavření smlouvy.

5.1 Získání formulářů

Zákazník si stáhne z webových stránek QCA formulář objednávky a formulář seznamu žadatelů. Dokumenty mu také může zaslat obchodní nebo kontaktní místo.

5.2 Vyplnění objednávky

Formulář objednávky vyplňte podle těchto pokynů:

- V bodu **1** jsou v sekci **Poskytovatel** automaticky nastaveny údaje o odštěpném závodě ČP, s nímž budete uzavírat smlouvu. Pouze podle adresy zkontrolujte, zda máte staženou správnou verzi objednávky. V sekci **Zákazník** zadejte obchodní údaje o vaší organizaci.
- V bodu **2** zaškrtněte, zda chcete uzavřít smlouvu na dobu určitou nebo neurčitou. Běžně se smlouva uzavírá na dobu neurčitou.
- V bodu **3** zaškrtněte, o jaké certifikáty hodláte žádat (kvalifikované a/nebo komerční). Můžete zaškrtnout jedno nebo obě políčka.
- V bodu **4.4** zvolte, zda hodláte udělit souhlas s využíváním kontaktních údajů vaší organizace za účelem marketingu a propagace produktů a služeb ČP. Zaškrtnutí políčka znamená, že tento souhlas neudělujete.
- Do bodu **5** se doplní identifikační údaje statutárního zástupce, místo a datum.

- V **příloze 1** objednávky určíte seznam oprávněných osob, které budou za organizaci jednat s QCA. Specifikujte jméno a příjmení každé oprávněné osoby a její rodné číslo.

Vyplněná objednávka se vytiskne ve dvou exemplářích. Oprávněné osoby stvrdí svým podpisem na příloze objednávky, že udělují České poště souhlas se zpracováním svých osobních údajů. Statutární zástupce organizace podepíše oba exempláře objednávky a přílohy objednávky.

Není vyžadováno ověření podpisů (notářem ani jiným způsobem).

Poznámka:

V případě organizací s malým počtem zaměstnanců může být oprávněnou osobou přímo statutární zástupce (a zřejmě i jedinou). Ve „velkých“ organizacích je naopak nanejvýš vhodné zvolit jako oprávněnou osobu někoho jiného, například zaměstnance z personálního oddělení v každé organizační jednotce organizace.

5.3 Doručení objednávky na obchodní/kontaktní místo

5.3.1 Doručení poštou

Poštou zašlete na obchodní či kontaktní místo vyplněnou a podepsanou objednávku.

Pokud **je** vaše organizace **zapsána v obchodním rejstříku**, k objednávce připojíte:

- originál výpisu z obchodního rejstříku (ne starší než 3 měsíce), *nebo*
- notářsky ověřenou kopii výpisu z obchodního rejstříku (originál nesmí být starší než 3 měsíce).

Pokud **není** vaše organizace **zapsána v obchodním rejstříku**, k objednávce připojíte:

- originál jiného dokumentu, v němž je stanoven statutární zástupce a IČ organizace, *nebo*
- notářsky ověřenou kopii jiného dokumentu, v němž je stanoven statutární zástupce a IČ organizace.

5.3.2 Doručení osobní návštěvou oprávněné osoby zákazníka

Mnohem vhodnější a rychlejší variantou je osobní návštěva oprávněné osoby zákazníka na obchodním či kontaktním místě.

Oprávněná osoba s sebou přinese vyplněnou a podepsanou objednávku.

Pokud **je** vaše organizace **zapsána v obchodním rejstříku**, k objednávce připojíte:

- originál výpisu z obchodního rejstříku (ne starší než 3 měsíce), *nebo*
- notářsky ověřenou kopii výpisu z obchodního rejstříku (originál nesmí být starší než 3 měsíce).

Pokud **není** vaše organizace **zapsána v obchodním rejstříku**, k objednávce připojíte:

- originál jiného dokumentu, v němž je stanoven statutární zástupce a IČ organizace, *nebo*
- notářsky ověřenou kopii jiného dokumentu, v němž je stanoven statutární zástupce a IČ organizace.

Pro oprávněnou osobu bude výhodnější, pokud spolu s objednávkou předá zároveň připravené seznamy žadatelů (viz kapitoly 5.5 a 5.6).

5.4 Akceptace objednávky ze strany ČP

5.4.1 V případě doručení objednávky poštou

Pokud operátor OM/RA obdrží od zákazníka podklady pro uzavření smlouvy poštou, zkontroluje údaje v dokumentech a v případě správnosti akceptuje objednávku. Následně informuje oprávněnou osobu zákazníka, že smlouva byla uzavřena a že se může dostavit s vyplněnými seznamy žadatelů (viz kapitoly 5.5 a 5.6). Zákazník obdrží podepsanou akceptaci objednávky poštou.

5.4.2 V případě doručení objednávky osobně oprávněnou osobou zákazníka

Pokud podklady pro uzavření smlouvy přinese osobně oprávněná osoba zákazníka, operátor OM/RA zkontroluje údaje v dokumentech a v případě správnosti akceptuje objednávku. Oprávněná osoba obdrží od operátora OM/RA jeden exemplář podepsané objednávky. Pokud oprávněná osoba přinesla seznamy žadatelů, provede se postup v kapitole 5.6.

5.5 Vyplnění seznamů žadatelů

V seznamu žadatelů si organizace určuje, jaké certifikáty budou vydány kterým zaměstnancům.

Formulář seznamu žadatelů se skládá z několika souborů, v nichž se nachází

- úvodní list seznamu žadatelů,
- přílohy pro vydání certifikátů žadatelům podle jednotlivých certifikačních politik,
- změnové přílohy pro správu žadatelů a vydávaných certifikátů (změna údajů žadatele nebo v certifikátu, zablokování či vyřazení žadatele, ukončení vydávání certifikátu).

Součástí výsledného seznamu žadatelů je vždy úvodní list a libovolný počet příloh.

Seznamy žadatelů vyplňují oprávněné osoby následovně:

5.5.1 Úvodní list seznamu žadatelů

- Jako první údaj doplňte „Evidenční číslo smlouvy“. Tento údaj naleznete v uzavřené smlouvě, doplnilo jej obchodní místo. Není-li smlouva ještě uzavřena, ponechte položku prázdnou.
- V bodu **1** doplňte informace o vaší organizaci (tytéž jako na objednávce).
- V bodu **2** doplňte identifikační údaje oprávněné osoby, která připravuje seznam žadatelů.
- V bodu **3** doplňte počet vytvořených příloh seznamu žadatelů.

Nakonec se úvodní list vytiskne. Zatím jej však oprávněná osoba nepodepisuje.

5.5.2 Příloha seznamu žadatelů Certifikáty pro ověření el. podpisu zaměstnance

- Jako první údaj vyplňte číslo přílohy.
- Dále doplňte „Evidenční číslo smlouvy“. Tento údaj naleznete v uzavřené smlouvě, doplnilo jej obchodní místo. Není-li smlouva ještě uzavřena, ponechte položku prázdnou.

- V první tabulce doplňte identifikační údaje o žadateli – jméno a příjmení a rodné číslo.
- V druhé tabulce doplňte povinné údaje certifikátu. Do údaje CN uveďte jméno a příjmení žadatele. Do údaje OU uveďte číslo zaměstnance v organizaci. Pokud nepoužíváte v organizaci zaměstnanecká čísla (nebo je nechcete uvádět do certifikátů), vytvořte si pro tyto účely speciální číslování. Každý zaměstnanec musí mít přiděleno jedinečné číslo; nesmí se vyskytnout dva zaměstnanci se stejným číslem. Jako poslední povinný údaj uveďte e-mailovou adresu zaměstnance.
- Stále v druhé tabulce můžete volitelně doplnit nepovinné údaje – jméno organizační jednotky (jméno oddělení nebo jméno pobočky) a funkci v organizaci (tj. pracovní pozici). Libovolný z údajů ale také můžete ponechat prázdný.
- Pod tabulkami se dále zaškrťává, zda má být certifikát zveřejněn na webových stránkách a na LDAP serveru QCA. Zaškrtnutí políčka znamená, že certifikát nebude veřejně přístupný. Spíše však doporučujeme povolit zveřejnění certifikátu (tj. nechat políčko nezaškrtnuté).
- Dále se zaškrťává, zda má certifikát obsahovat Identifikátor klienta MPSV. Pokud hodláte komunikovat se státní správou, doporučujeme políčko zaškrtnout. Přidělení identifikátoru není zpoplatňováno.
- Pokud žadatel zaškrtl, že požaduje Identifikátor klienta MPSV, musí vyplnit druhou stránku přílohy. Zde se nachází formulář, v němž uděluje souhlas s poskytnutím osobních údajů pro MPSV. Vyplnění a podepsání formuláře je podmínkou pro přidělení identifikátoru MPSV.

Příloha seznamu žadatelů se vytiskne a podepíše ji příslušný žadatel. Formulář pro MPSV se musí vytisknout na samostatný papír, nepoužívejte proto oboustranný tisk.

5.5.3 Příloha seznamu žadatelů Certifikáty pro ověření el. značky organizace

- Jako první údaj vyplňte číslo přílohy.
- Dále doplňte „Evidenční číslo smlouvy“. Tento údaj naleznete v uzavřené smlouvě, doplnilo jej obchodní místo. Není-li smlouva ještě uzavřena, ponechte položku prázdnou.
- V první tabulce doplňte identifikační údaje o žadateli – jméno a příjmení, rodné číslo a číslo žadatele v organizaci. Pokud nepoužíváte v organizaci zaměstnanecká čísla (nebo je nechcete uvádět do certifikátů), vytvořte si pro tyto účely speciální číslování. Každý zaměstnanec musí mít přiděleno jedinečné číslo; nesmí se vyskytnout dva zaměstnanci se stejným číslem.
- V druhé tabulce doplňte povinný údaj certifikátu CN – uveďte sem jméno certifikátu pro označující zařízení.
- Stále v druhé tabulce můžete volitelně doplnit nepovinné údaje – jméno organizační jednotky (jméno oddělení nebo jméno pobočky) a e-mailovou adresu. Libovolný z údajů ale také můžete ponechat prázdný. E-mailovou adresu silně doporučujeme vyplnit!
- Pod tabulkami se dále zaškrťává, zda má být certifikát zveřejněn na webových stránkách a na LDAP serveru QCA. Zaškrtnutí políčka znamená, že certifikát nebude veřejně přístupný. Spíše však doporučujeme povolit zveřejnění certifikátu (tj. nechat políčko nezaškrtnuté).

Příloha seznamu žadatelů se vytiskne a podepíše ji příslušný žadatel.

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

(Předpokládáme však, že zákazníci většinou nebudou požadovat vydání kvalifikovaných systémových certifikátů s doménovými jmény.)

5.5.4 Změnová příloha seznamu žadatelů Certifikáty pro ověření el. podpisu zaměstnance

- Jako první údaj vyplňte číslo přílohy.
- Dále doplňte „Evidenční číslo smlouvy“. Tento údaj naleznete v uzavřené smlouvě, doplnilo jej obchodní místo. Není-li smlouva ještě uzavřena, ponechte položku prázdnou.
- V první tabulce doplňte identifikační údaje o žadateli, kterému je příslušný certifikát vydáván – jméno a příjmení a rodné číslo.
- V druhé tabulce doplňte stávající znění povinných a nepovinných údajů příslušného certifikátu.
- V části Správa údajů o žadateli máte možnost změnit osobní údaje žadatele, zablokovat žadatele, odblokovat zablokovaného žadatele nebo zcela vyřadit žadatele ze systému QCA.
- V části Správa údajů o certifikátu máte možnost změnit údaje certifikátu, změnit zveřejnění certifikátu, změnit vkládání Identifikátoru MPSV do certifikátu nebo zcela zrušit vydávání certifikátu žadateli. Pokud požadujete vložení Identifikátoru klienta MPSV do certifikátu, je potřeba vyplnit třetí stránku přílohy. Zde se nachází formulář, v němž žadatel uděluje souhlas s poskytnutím osobních údajů pro MPSV. Vyplnění a podepsání formuláře je podmínkou pro přidělení identifikátoru MPSV.

Vytištěnou přílohu nakonec podepíše žadatel. Za určitých okolností může přílohu podepsat také oprávněná osoba, což je blíže vysvětleno na formuláři přílohy.

5.5.5 Změnová příloha seznamu žadatelů Certifikáty pro ověření el. značky organizace

- Jako první údaj vyplňte číslo přílohy.
- Dále doplňte „Evidenční číslo smlouvy“. Tento údaj naleznete v uzavřené smlouvě, doplnilo jej obchodní místo. Není-li smlouva ještě uzavřena, ponechte položku prázdnou.
- V první tabulce doplňte identifikační údaje o žadateli, kterému je příslušný certifikát vydáván – jméno a příjmení, rodné číslo a číslo žadatele v organizaci.
- V druhé tabulce doplňte stávající znění povinných a nepovinných údajů příslušného certifikátu.
- V části Správa údajů o žadateli máte možnost změnit osobní údaje žadatele, zablokovat žadatele, odblokovat zablokovaného žadatele nebo zcela vyřadit žadatele ze systému QCA.

- V části Správa údajů o certifikátu máte možnost změnit údaje certifikátu, změnit zveřejnění certifikátu nebo zcela zrušit vydávání certifikátu žadateli.

Vytisknutou přílohu nakonec podepíše žadatel. Za určitých okolností může přílohu podepsat také oprávněná osoba, což je blíže vysvětleno na formuláři přílohy.

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

(Předpokládáme však, že zákazníci většinou nebudou požadovat vydání kvalifikovaných systémových certifikátů s doménovými jmény.)

5.6 Doručení prvního seznamu žadatelů na obchodní nebo kontaktní místo

Doručení seznamu žadatelů závisí na zvoleném způsobu ověření podpisu oprávněné osoby:

- Oprávněná osoba podepíše seznam žadatelů před notářem (tzv. notářsky ověřený podpis). Seznam žadatelů se zašle na **obchodní místo** poštou. V tomto případě hradíte notáři poplatek za ověření podpisu.
- Oprávněná osoba se dostaví se seznamem žadatelů na **obchodní či kontaktní místo** osobně a podepíše se před pracovníkem ČP (tzv. podpis ověřený pracovníkem ČP). V tomto případě je ověření podpisu bezplatné.
- Vlastní-li oprávněná osoba certifikát vydaný certifikační autoritou České pošty (tj. PostSignum QCA nebo PostSignum VCA), může zaslat na **obchodní místo** elektronickou verzi seznamu žadatelů podepsaným e-mailem. Musí však zároveň poslat poštou podepsaný papírový originál seznamu žadatelů (z důvodu písemného souhlasu žadatelů se zpracováním jejich osobních údajů Českou poštou).

Obchodní místo převezme seznamy žadatelů a žadatele zavede do systému QCA. Během tohoto procesu již není nutná přítomnost oprávněné osoby, o zavedení všech žadatelů do systému QCA je informována e-mailem nebo telefonicky. Poté se mohou příslušní žadatelé dostavit na kontaktní místo nechat si vydat certifikát.

Kontaktní místo může seznam žadatelů zpracovat pouze v případě tzv. zrychleného zavedení zákazníka do systému (viz kapitola 4.4). Jinak může kontaktní místo dokument pouze zaslat ke zpracování na obchodní místo.

5.7 Doručení dalších seznamů žadatelů

Příprava dalších seznamů žadatelů může být potřeba z těchto důvodů:

- organizace chce nechat vydat certifikáty novým žadatelům
- organizace požaduje změnu údajů ve stávajících vydaných certifikátech nebo ukončit jejich vydávání žadatelům
- došlo ke změně osobních údajů stávajících žadatelů
- vyřazení žadatelů se seznamu žadatelů

Oprávněná osoba má opět tři možnosti doručení seznamů žadatelů v závislosti na zvoleném způsobu ověření podpisu oprávněné osoby, které již byly popsány v kapitole 5.6.

Další seznamy žadatelů může zpracovat pouze obchodní místo, proto po ověření podpisu oprávněné osoby pracovníkem ČP na kontaktním místě se dokument odesílá na obchodní místo, což znamená určitou časovou prodlevu.

O zavedení všech žadatelů do systému QCA je oprávněná osoba informována e-mailem nebo telefonicky.

5.8 Změna uzavřené smlouvy s Českou poštou

V případě změny obchodních údajů organizace, seznamu oprávněných osob nebo jiných ustanovení ve smlouvě je uzavřen s obchodním místem dodatek ke smlouvě.

6 Vydání certifikátů žadatelům

6.1 Vygenerování klíčů a elektronické žádosti o certifikát

Před vydáním certifikátu si žadatel musí na svém počítači vygenerovat klíčový pár a elektronickou žádost o certifikát. Pro tyto účely jsou na webových stránkách QCA nabízeny příslušné nástroje. Na webových stránkách si dále můžete stáhnout příručky popisující postupy generování klíčů v těchto nástrojích.

6.2 Vydání certifikátu zaměstnanci organizace

Žadatel o certifikát se dostaví na kontaktní místo s jedním platným dokladem totožnosti (občanský průkaz nebo cestovní pas) a disketou s elektronickou žádostí o certifikát. V průběhu vydávání certifikátu ověří operátor RA identitu žadatele. Zkopíruje osobní doklad žadatele, což stanovuje zákon č.227/2000 Sb. o elektronickém podpisu.

Vytiskne se písemná žádost o certifikát, kterou žadatel svým podpisem schválí.

Na žádosti se uvádí tzv. heslo pro zneplatnění, které souvisí s procesem zneplatnění certifikátu (viz kapitola 6.4). Toto heslo určuje žadatel. Není nutné si je pamatovat, protože bude uvedeno v protokolu o vydání certifikátu. Heslo by se nemělo shodovat s jinými hesly, která žadatel běžně používá.

Po vydání certifikátu žadatel přijme vydaný certifikát. Následně je vystaven protokol o vydání certifikátu. Žadateli je na disketu nakopírován vydaný certifikát, certifikáty a CRL certifikačních autorit a certifikační politika ve formátu PDF, podle níž byl certifikát vystaven.

Žadatel má také právo vydaný certifikát odmítnout. V tom případě je vytištěn protokol o nevydání certifikátu a certifikát je zneplatněn.

Pozor! V případě odmítnutí vydaného certifikátu nemůže být okamžitě vydán nový certifikát. Žadatel si musí vygenerovat nový klíčový pár a žádost o certifikát a navštívit kontaktní místo znovu.

6.3 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 QCA. Naleznete je na disketě s vydaným certifikátem nebo na webových stránkách PostSignum QCA.

Poznámka: V případě e-mailových klientů Outlook/Outlook Express je potřeba nainstalovat všechny certifikáty (a klíče) do operačního systému Windows; v ostatních případech pravděpodobně přímo do cílových aplikací.

Postupy instalace vydaného certifikátu a certifikátů certifikačních autorit jsou součástí příruček, které popisují generování klíčů a žádostí o certifikát. Tyto příručky můžete stáhnout z webových stránek QCA.

6.4 Zneplatnění certifikátu

Může dojít k situaci, kdy žadatel již nemůže 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 je potřeba požádat o zneplatnění certifikátu, který odpovídá prozrazenému (ztracenému) soukromému klíči.

Žádost o zneplatnění se podává na kontaktním místě. Pracoviště může žadatel navštívit osobně nebo kontaktovat telefonicky či e-mailem. Aby bylo možné identifikovat správný certifikát, musí operátorce sdělit sériové číslo certifikátu, nebo jméno certifikátu a datum vystavení. Tyto údaje nalezne v protokolu o vydání certifikátu. Žadatel musí sdělit, která certifikační autorita certifikát vydala – QCA nebo VCA.

Operátorce dále žadatel sdělí heslo pro zneplatnění, které je opět uvedeno v protokolu o vydání certifikátu. Tímto se ověří, zda-li má oprávnění žádat o zneplatnění daného certifikátu. Pokud heslo nesouhlasí, nebo je žadatel nezná, musí se na kontaktní místo dostavit osobně (s platným dokladem totožnosti) a vyplnit písemnou žádost o zneplatnění certifikátu (vzor žádosti lze stáhnout z webových stránek QCA). Certifikát je zneplatněn po ověření dokladu. Doklad je opět zkopírován, stejně jako při vydávání certifikátu. Na konci procesu žadatel obdrží protokol o zneplatnění certifikátu.

Mimo pracovní dobu kontaktních míst lze telefonicky či e-mailem kontaktovat tzv. Nonstop zneplatňující službu (kontaktní údaje jsou uvedeny na webových stránkách QCA). I zde je nutné sdělit stejné údaje o certifikátu a heslo pro zneplatnění. Nebude-li heslo pro zneplatnění úspěšně ověřeno, pracovníci doporučí žadateli návštěvu kontaktního místa během pracovní doby.

O zneplatnění certifikátů, vydaných žadatelům (zaměstnancům organizace), mohou žádat také **oprávněné osoby**. Oprávněná osoba připraví žádost o zneplatnění certifikátu - formulář žádosti je k dispozici na webových stránkách QCA. Žádost se České poště doručí jedním z těchto způsobů:

- Oprávněná osoba žádost vytiskne a podepíše. Se žádostí a dokladem totožnosti se dostaví osobně na nejbližší kontaktní místo, kde proběhne zneplatnění certifikátu.
- Oprávněná osoba žádost vytiskne a podepíše. Žádost odešle poštou nebo faxem na adresu centra QCA. (Mimo pracovní dobu centra QCA pošlete žádost na faxové číslo nonstop zneplatňující služby.)

- Oprávněná osoba odešle vyplněný elektronický dokument se žádostí podepsaným e-mailem na e-mailovou adresu centra QCA. (Oprávněná osoba musí mít „osobní“ certifikát vydaný certifikační autoritou PostSignum QCA nebo PostSignum VCA.)

Není vyžadováno ověření podpisu na papírové žádosti (notářem ani jiným způsobem). Kontaktní údaje centra QCA, nonstop zneplatňující služby a kontaktních míst jsou k dispozici na webových stránkách QCA.

7 Ostatní

7.1 Fakturace

Ceník služeb QCA je součástí uzavřené smlouvy. Aktuální verze ceníku je k dispozici na webových stránkách QCA.

Cena za služby QCA je fakturována podle platného ceníku a smlouvy vždy podle počtu vydaných certifikátů. V případě, že nebyly vydány žádné certifikáty, není faktura vystavována. Faktura je zasílána na adresu uvedenou ve smlouvě.

7.2 Platnost certifikátu a jeho obnova

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

Pokud nedošlo ke změně údajů žadatele nebo v certifikátu, je možné opět si nechat vystavit nový certifikát osobně na kontaktním místě podle postupu popsaného v kapitole 6.1.

Kromě osobní návštěvy je také možné elektronickou cestou požádat o vydání následného certifikátu. Žadatel pošle na adresu elektronické podatelny PostSignum elektronicky podepsaný e-mail se žádostí o vydání certifikátu.

Pokud došlo ke změně údajů, doručí oprávněná osoba obchodnímu místu „změnové“ seznamy žadatelů (použijí se změnové přílohy). Obchodní místo provede příslušné změny v systému QCA a informuje oprávněnou osobu o provedení změn. Poté se mohou žadatelé dostavit na kontaktní místo nechat si vydat nový certifikát.

Obnova certifikátu je opět zpoplatněna formou faktury. Cena certifikátu je stanovena podle aktuálně platného ceníku.

8 Názorný příklad

Jakákoliv podobnost se skutečnými organizacemi a osobami je čistě náhodná a neúmyslná.

8.1 Informace o fiktivní firmě

Firma **První distribuční, a.s.** s centrálou v **Praze** a pobočkami v **Brně** a **Ostravě** se rozhodla, že začne využívat služeb QCA.

Managementu budou vystaveny kvalifikované certifikáty, které se budou používat pro komunikaci se státní správou. Dále bylo stanoveno, že firma při obchodní komunikaci s partnery bude vyžadovat podpis kvalifikovaným certifikátem.

Firma si také nechá vystavit kvalifikovaný systémový certifikát pro svůj „auto-responder“, aplikaci posílající automatické potvrzení o došlých e-mailových zprávách od obchodních partnerů.

Tento příklad lze aplikovat jak na organizace komunikující se státní správou, tak na samotné orgány státní správy.

8.2 Uzavření smlouvy o poskytování certifikačních služeb

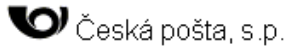
8.2.1 Příprava objednávky

Vyřízením smlouvy pověřil generální ředitel **Oldřich Bass** svého technického náměstka **Josefa Drobného**.

Ten si stáhl z webových stránek <http://qca.postsignum.cz> vzor objednávky pro právnické osoby. Po prostudování dokumentu se rozhodl, že:

- smlouvu uzavře na dobu neurčitou,
- firma bude objednávat služby vydání certifikátů kvalifikovanou i komerční autoritou (v budoucnu se to může hodit),
- poskytne souhlas s používáním kontaktních údajů firmy pro marketingové účely ČP (jedná se o dopravní firmu a je dobré vědět, jaké nové služby ČP nabízí),
- oprávněnou osobu pro pražskou centrálu stanoví sebe, pro brněnskou pobočku technického náměstka **Arnošta Zíku** a pro ostravskou pobočku vedoucí personálního oddělení **Ivetu Vondrášovou**.

Vyplněná objednávka vypadala následovně:



OBJEDNÁVKA POSKYTOVÁNÍ SLUŽEB CERTIFIKAČNÍ AUTORITY

Evidenční číslo smlouvy (objednávky):

1. Smluvní strany

Poskytovatel

Česká pošta, s.p., Olšanská 38/9, Praha 3
zastoupená:
odštěpný závod Střední Čechy
se sídlem Politických vězňů 909/4, 115 00 Praha 1
IČ: 47114983 DIČ: CZ47114983
zapsaná v obchodním rejstříku, vedeném u Městského soudu v Praze, sp. zn. A 7566
Bankovní spojení ČSOB, a.s., č.ú.133406370/0300

Zákazník

Firma **První distribuční, a.s.**
zastoupená **Oldřichem Bassem**
Organizační jednotka
se sídlem **Vitavská 35, 150 00 Praha 5**
IČ: **12345678** DIČ: **CZ12345678**
zapsaná v **obchodním rejstříku vedeném u Městského soudu v Praze, sp.zn. C 1456**
Bankovní spojení **Fiktivní banka, a.s., č.ú. 1234567890/0111**

2. Trvání smlouvy

Tato smlouva se uzavírá na dobu neurčitou
 dobu určitou od do

3. Objednávané služby

Certifikáty vydávané kvalifikovanou certifikační autoritou PostSignum: →

- certifikát určený k ověření elektronického podpisu zaměstnance (kvalifikovaný certifikát)
- certifikát organizace určený pro ověření elektronické značky (kvalifikovaný systémový certifikát)

Certifikáty vydávané komerční certifikační autoritou PostSignum: →

- certifikát technologických komponent (komerční certifikát)
- šifrovací certifikát skupiny osob (komerční certifikát)
- certifikát zaměstnanců nebo podnikajících fyzických osob (komerční certifikát)



4. Společná a závěrečná ustanovení

4.1 Dne 3.8.2005 se na základě rozhodnutí Ministerstva informatiky ČR stala Česká pošta, s.p. akreditovaným poskytovatelem certifikačních služeb ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu.

4.2 Podpisem této objednávky potvrzujete, že jste se podrobně seznámili s aktuálním zněním Smlouvy a všech jejích součástí, které jsou: Všeobecné obchodní podmínky, Popis služeb certifikační autority - Certifikační politiky, Ceník, Zákaznické formuláře. Před podáním této objednávky si prostudujte další součásti Smlouvy. Aktuální znění výše uvedených smluvních dokumentů naleznete na www.postsignum.cz a dále na všech kontaktních místech poskytovatele určených pro styk s veřejností. Adresy těchto kontaktních míst jsou uvedeny na www.postsignum.cz.

4.3 Změny v popisu služeb certifikační autority, ceníku a zákaznických formulářích nepodléhají udělení písemnému souhlasu ze strany zákazníka. Plánované změny těchto dokumentů budou v předstihu zveřejněny na www.postsignum.cz.

4.4 V případě, že nehodláte ve smyslu čl.7, odst.2b, Všeobecných obchodních podmínek, udělit poskytovateli svůj souhlas se zpracováním vašich osobních údajů za účelem marketingu či propagace produktů a služeb poskytovatele, zaškrtněte

4.5 Reklamační služby poskytované se provádí výhradně v místě poskytnutí služby. Poskyvatel sepíše se zákazníkem reklamační protokol. V případě oprávněné reklamacie bude sjednána náprava nejpozději do 14 dnů od sepsání reklamačního protokolu. V případě neoprávněné reklamacie bude zákazník poskytovatelem informován o důvodu neuznání reklamacie.

4.6 Spory, které z tohoto vztahu vzniknou, se řeší u věcně a místně příslušného soudu.

4.7 S touto objednávkou předává zákazník seznam oprávněných osob, které jsou oprávněny s poskytovatelem jednat ve věci služeb, které jsou předmětem uzavírané smlouvy.

4.8 Tato objednávka je vyhotovena ve dvou stejnopisech. Každá smluvní strana obdrží jedno vyhotovení objednávky.

4.9 Akceptací vámi podepsané objednávky ze strany poskytovatele dojde k uzavření smlouvy o poskytování služeb certifikační autority PostSignum.

5. Podpisy smluvních stran

Za poskytovatele

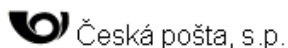
..... Místo Datum

..... Jméno a příjmení Podpis a razítko

Za zákazníka

Praha **1.9.2006**
..... Místo Datum

Oldřich Bass
..... Jméno a příjmení Podpis a razítko



Příloha č.1 Objednávky poskytování služeb certifikační autority

Evidenční číslo smlouvy (objednávky):

Seznam oprávněných osob

Údaje o oprávněných osobách

Jméno a příjmení	Rodné číslo	Podpis
Josef Drobný	123456/1234	
Arnošt Zíka	999999/8888	
Iveta Vondrášová	111111/2222	
■	■	
■	■	
■	■	
■	■	
■	■	
■	■	
■	■	
■	■	
■	■	
■	■	
■	■	
■	■	

Oprávněné osoby svým podpisem souhlasí s poskytnutím osobních údajů certifikační autoritě poskytovatele za účelem prokázání totožnosti v rozsahu jméno, příjmení a rodné číslo. Souhlas se uděluje na dobu trvání smluvního vztahu.

Oprávněné osoby svým podpisem prohlašují, že byly poučeny ve smyslu § 11 a 12 zákona č. 101/2000 Sb., v tom smyslu, že povinnost poskytnout osobní údaje uvedené v tiskopisu nevyplývá ze zvláštních zákonů, ale jejich poskytnutí je dobrovolné. Oprávněné osoby berou na vědomí, že pokud tyto informace neuvedou, nemohou být zákazníkovi ze strany poskytovatele poskytnuty požadované služby.

Oprávněné osoby dále berou na vědomí informace o svém právu na přístup k osobním údajům, které jsou zpracované za účelem poskytnutí požadovaných služeb zákazníkovi, právu na opravu těchto osobních údajů i povinnosti poskytovatele na požádání oprávněným osobám sdělit informace o jejich zpracování, jakož i o dalších právech stanovených v §21 zákona č. 101/2000 Sb.

Podpisy smluvních stran:

.....
Za zákazníka

.....
Za poskytovatele

Objednávku **Josef Drobný** vytiskl ve dvou exemplářích. Dvakrát vytištěnou přílohu objednávky poslal poštou ostatním oprávněným osobám k podepsání a počkal na vrácení podepsané přílohy, na kterou nakonec přidal i svůj podpis. Oba exempláře objednávky a přílohy nechal podepsat generálním ředitelem.

8.3 Příprava seznamů žadatelů

Josef Drobný se rozhodl, že pro začátek bude vystaven certifikát pouze pro něj a že certifikát pro „auto-responder“ vyzvedne vedoucí administrátor **Miroslav Táborský**.

Z adresy <http://qca.postsignum.cz> si stáhl vzor úvodního listu seznamu žadatelů, přílohu pro politiku „Certifikáty pro ověření elektronického podpisu zaměstnance“ (ta bude pro něj) a přílohu pro politiku „Certifikáty organizace pro ověření elektronické značky“ (ta bude pro administrátora).

8.3.1 Vyplnění úvodního listu seznamu žadatelů

Josef Drobný ponechal v záhlaví úvodního listu nevyplněné evidenční číslo smlouvy, protože ještě není smlouva uzavřena. Doplnil údaje o firmě a jako oprávněnou osobu uvedl sebe. Jako počet příloh uvedl 2. Vyplněný úvodní list vypadal následovně:

Seznam žadatelů zákazníka

Evidenční číslo smlouvy (objednávky):

1. Údaje o zákazníkovi

Firma První distribuční, a.s.
IČ 12345678

2. Údaje o oprávněné osobě

Jméno a příjmení Josef Drobny
Kontaktní telefon 123 456 789
Kontaktní e-mail drobny@1distribucni.cz

3. Údaje o žadatelích

Oprávněná osoba žádá, aby byly do evidence certifikační autority České pošty zaznamenány údaje žadatelů, jejichž údaje jsou uvedeny na jednotlivých číslovaných přílohách.

Počet příloh 2

4. Podpis oprávněné osoby ¹⁾

..... Místo Datum Podpis

5. Ověření podpisu oprávněné osoby pracovníkem České pošty, s.p. ¹⁾

Jméno a příjmení ověřovatele

Datum a podpis ověřovatele

¹⁾ Pokud má oprávněná osoba kvalifikovaný certifikát nebo podpisový certifikát vydaný certifikační autoritou České pošty, nemusí se dostavit osobně, ale může tento formulář včetně příloh poslat elektronicky a podepsat jej platným certifikátem. Zároveň je však nutné poslat formulář s přílohami i písemně s podpisy všech žadatelů uvedených na formuláři, aby mohly být zpracovány jejich osobní údaje v souladu se zákonem č. 101/2000 Sb.

Zákaznické formuláře: zákazník - organizace

Úvodní list poté vytiskl. Nepodepisoval jej.

8.3.2 Vyplnění přílohy seznamu žadatelů Certifikáty pro ověření elektronického podpisu zaměstnance

Dále začal vyplňovat přílohu pro politiku „Certifikáty pro ověření elektronického podpisu zaměstnance.“ Bez problémů zadal své jméno a příjmení a rodné číslo.

Dále vyplnil údaje certifikátu. Jako údaj CN zadal své **jméno a příjmení**. Do údaje „číslo žadatele v organizaci“ zadal své **zaměstnanecké číslo**. Dále zadal svoji e-mailovou adresu. U údaje „organizační jednotka“ chvíli zapřemýšlel. Rozhodl se, že doplní text **Centrála Praha** a

na pobočky poslal pokyn, aby do tohoto údaje zaměstnanci doplňovali **Pobočka Brno**, respektive **Pobočka Ostrava**. Údaj „funkce v organizaci“ již zadal bez problémů. Dále povolil zveřejnění svého certifikátu, aby si jej mohli stáhnout komunikující partneři. Také požádal o uvedení „identifikátoru klienta MPSV“ v certifikátu. Vyplnil souhlas pro MPSV na druhé stránce. Vyplněná příloha vypadala následovně:

Příloha č. 1

Údaje pro vydání certifikátu určeného k ověření elektronického podpisu zaměstnance (kvalifikovaný certifikát)

Evidenční číslo smlouvy (objednávky):

Údaje o žadateli

Jméno a příjmení	Josef Drobny
Rodné číslo (pro občany ČR)	
Datum narození, číslo a typ dokladu (pro cizince)	123456/1234

Údaje o certifikátu

Povinné položky		
CN (jméno a příjmení, tituly)	(max. 100 znaků)	Josef Drobny
OU (číslo žadatele v organizaci)	(max. 20 znaků)	254
Adresa elektronické pošty	(max. 250 znaků)	drobny@1distribucni.cz
Nepovinné položky		
OU (org. jednotka, kde žadatel pracuje)*	(max. 200 zn.)	Centrála Praha
Funkce v organizaci*	(max. 100 znaků)	technický náměstek

* V souladu s odst. 2 § 1 Nařízení vlády č. 495/2004 Sb. musí být tyto položky povinně vyplněny v případě certifikátů pro zaměstnance orgánů veřejné moci.

V případě, že si nepřejete zveřejnění vydaného certifikátu nebo vydaných certifikátů na webových stránkách (adresářových službách) České pošty, zaškrtněte

Pokud jste nezaškrtnli okénko v předchozím odstavci, má se za to, že jste svým podpisem vyslovili svůj souhlas se zveřejněním údajů obsažených ve vydaném certifikátu nebo vydaných certifikátech.

Pokud si přejete, aby váš kvalifikovaný certifikát obsahoval identifikátor klienta Ministerstva práce a sociálních věcí, zaškrtněte

Žadatel svým podpisem stvrzuje, že souhlasí s poskytnutím svých osobních údajů certifikační autoritě České pošty a s jejich zpracováním za účelem vydání a správy certifikátů. Souhlas se uděluje na dobu 10 let od ukončení platnosti kvalifikovaného certifikátu (v souladu s §6 zákona č. 227/2000 Sb.).

Žadatel svým podpisem prohlašuje, že byl poučen ve smyslu § 11 a 12 zákona č. 101/2000 Sb., v tom smyslu, že povinnost poskytnout osobní údaje uvedené v tiskopisu nevyplývá ze zvláštních zákonů, ale jejich poskytnutí je dobrovolné. Žadatel bere na vědomí, že pokud tyto informace neuvede, nemůže mu být ze strany České pošty poskytnuta požadovaná služba.

Žadatel dále bere na vědomí informace o svém právu na přístup k osobním údajům, které jsou zpracovány za účelem poskytnutí jim požadované služby, právu na opravu těchto osobních údajů i povinnosti České pošty na požádání žadatele sdělit informace o jejich zpracování, jakož i o dalších právech stanovených v §21 zákona č. 101/2000 Sb.

Zaškrtnutím okénka, aby váš kvalifikovaný certifikát obsahoval identifikátor klienta Ministerstva práce a sociálních věcí, se na vás vztahují následující zvláštní ustanovení:

- Žadatel bere na vědomí, že Ministerstvo práce a sociálních věcí (dále jen „MPSV“) vede podle zákona č.117/1995 Sb., o státní sociální podpoře, ve znění pozdějších předpisů (dále jen „zákon o státní sociální podpoře“), informační systém o dávkách státní sociální podpory a jejich výši, o poživatelích těchto dávek a žadatelích o tyto dávky (dále jen „klient MPSV“) a osobách s nimi společně posuzovaných (dále jen „informační systém MPSV“).
- Žadatel - klient MPSV nebo budoucí klient MPSV svým podpisem stvrzuje, že mu byl MPSV prostřednictvím České pošty přidělen identifikátor klienta MPSV, který je umístěn v kvalifikovaném certifikátu a slouží výhradně pro ověření totožnosti žadatele – klienta MPSV v informačním systému MPSV při elektronické komunikaci žadatele – klienta MPSV a MPSV.
- Žadatel - klient MPSV nebo budoucí klient MPSV svým podpisem Souhlasu žadatele se zpracováním osobních údajů vyjadřuje souhlas v souladu s § 5 odst.5 zákona č.101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů s tím, že MPSV vede evidenci žadatelů – klientů MPSV nebo budoucích klientů MPSV, kterým byl Českou poštou vydán kvalifikovaný certifikát. Evidence je vedena výhradně pro účely prokázání totožnosti žadatele – klienta MPSV v případě jeho elektronické komunikace s MPSV podle zákona o státní sociální podpoře. Evidence obsahuje tyto údaje: jméno a příjmení žadatele, rodné číslo nebo ekvivalentní údaj, ze kterého je zřejmé pohlaví žadatele, titul před jménem a za příjmením žadatele, a adresu pobytu žadatele.

.....
Podpis žadatele

Zákaznické formuláře: zákazník – organizace



Česká pošta, s.p.

PostSignum QCA

Souhlas žadatele se zpracováním osobních údajů podle § 5 odst. 5 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů:

Zadatel souhlasí s tím, že MPSV bude pro účely prokázání totožnosti žadatele – klienta Informačního systému státní sociální podpory (IS SSP), resp. MPSV nebo budoucího klienta IS SSP, resp. MPSV pro případ jeho elektronické komunikace s MPSV podle zákona č. 117/1995 Sb., o státní sociální podpoře, v aktuálním znění, zpracovávat osobní údaje žadatele – klienta IS SSP, resp. MPSV nebo budoucího klienta IS SSP, resp. MPSV v rozsahu jméno a příjmení žadatele, rodné číslo nebo ekvivalentní údaj, ze kterého je zřejmé pohlaví žadatele, titul před jménem a za příjmením žadatele a adresu pobytu žadatele. Souhlas se uděluje na dobu neurčitou.

V Praze dne 4.9.2006

Žadatel

Jméno: Josef

Příjmení: Drobný

Datum narození: 1.1.1960

Adresa pobytu

Obec - město: Praha

Část obce:

Ulice: Pod Strání

Číslo: 1

PSČ: 111 00

Podpis

Pozn.: Tento Souhlas vyplňte pouze v případě, pokud si přejete, aby váš kvalifikovaný certifikát obsahoval identifikátor klienta Ministerstva práce a sociálních věcí. Souhlas je nutné vytisknout na samostatném listu.

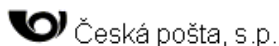
Zákaznické formuláře: zákazník – organizace

Přílohu nakonec jednou vytiskl a podepsal oba listy.

8.3.3 Vyplnění přílohy seznamu žadatelů pro politiku Certifikáty pro ověření elektronické značky organizace

Miroslav Táborský dostal za úkol vyplnit přílohu pro vydání certifikátu pro ověření elektronické značky. Snadno zadal své jméno a příjmení, rodné číslo a zaměstnanecké číslo. Pokračoval s vyplňováním údajů certifikátu. Jako jméno certifikátu bylo po větší diskusi s marketingovým oddělením a programátory vybráno **První distribuční - automatická odpověď**. Na pokyn **Josefa Drobného** použil v údajích „organizační jednotka“ jeho dělení, doplnil tedy **Centrála Praha**. Do údaje „e-mailová adresa“ doplnil **obchod@1distribucni.cz**, což je schránka, na kterou přichází obchodní komunikace.

Povolil zveřejnění certifikátu. Příloha nakonec vypadala takto:



PostSignum QCA

Příloha č. 2

Údaje pro vydání certifikátu organizace určeného pro ověření elektronické značky (kvalifikovaný systémový certifikát)

Evidenční číslo smlouvy (objednávky):

Údaje o žadateli

Jméno a příjmení	Miroslav Tábořský
Rodné číslo (pro občany ČR)	444444/5555
Datum narození, číslo a typ dokladu (pro cizince)	
Číslo žadatele v organizaci (max. 20 znaků)	722

Údaje o certifikátu

Povinné položky	
CN (jméno označujícího zařízení) (max. 100 znaků)	První distribuční - automatická odpověď
Nepovinné položky	
OU (organizační jednotka, kde je označující zařízení umístěno) (max. 200 znaků)	Centrála Praha
Adresa elektronické pošty* (max. 250 znaků)	obchod@1distribucni.cz

* Důrazně doporučujeme vyplnění adresy elektronické pošty, přestože se jedná o nepovinný údaj. Certifikát bez (správné) e-mailové adresy nelze použít pro odesílání podepsaných e-mailových zpráv.

V případě, že si nepřejete zveřejnění vydaného certifikátu nebo vydaných certifikátů na webových stránkách (adresářových službách) České pošty, zaškrtněte →

Pokud jste nezaškrtnli okénko v předchozím odstavci, má se za to, že jste svým podpisem vyslovili svůj souhlas se zveřejněním údajů obsažených ve vydaném certifikátu nebo vydaných certifikátech.

Zadatel svým podpisem stvrzuje, že souhlasí s poskytnutím svých osobních údajů certifikační autoritě České poště a s jejich zpracováním za účelem vydání a správy certifikátů. Souhlas se uděluje na dobu 10 let od ukončení platnosti kvalifikovaného certifikátu (v souladu s §6 zákona č. 227/2000 Sb.).

Žadatel svým podpisem prohlašuje, že byl poučen ve smyslu § 11 a 12 zákona č. 101/2000 Sb., v tom smyslu, že povinnost poskytnout osobní údaje uvedené v tiskopisu nevyplývá ze zvláštních zákonů, ale jejich poskytnutí je dobrovolné. Žadatel bere na vědomí, že pokud tyto informace neuvede, nemůže mu být ze strany České pošty poskytnuta požadovaná služba.

Žadatel dále bere na vědomí informace o svém právu na přístup k osobním údajům, které jsou zpracovány za účelem poskytnutí jim požadované služby, právu na opravu těchto osobních údajů i povinnosti České pošty na požádání žadatele sdělit informace o jejich zpracování, jakož i o dalších právech stanovených v §21 zákona č. 101/2000 Sb.

.....
Podpis žadatele

Zákaznické formuláře: zákazník – organizace

Přílohu vytiskl a podepsal.

8.4 Doručení objednávky a seznamu žadatelů na obchodní místo

Josef Drobný si s obchodním místem domluvil osobní schůzku a s sebou přinesl

- vytištěnou a podepsanou objednávku ve dvou exemplářích (včetně vytištěné a podepsané přílohy objednávky ve dvou formulářích),
- výpis z obchodního rejstříku,
- vytištěný a žadateli podepsaný seznam žadatelů,
- svůj doklad totožnosti.

Operátorka obchodního místa zkontrolovala vyplněné objednávky, zkopírovala si výpis z obchodního rejstříku a uzavřela smlouvu. **Josef Drobný** obdržel jeden podepsaný exemplář objednávky a přílohy objednávky.

Operátorka dále ověřila identitu **Josefa Drobného** vůči osobnímu dokladu. Ten se před operátorkou se podepsal jako oprávněná osoba na úvodní list seznamu žadatelů a operátorka potvrdila ověření podpisu na úvodním listu. Nakonec **Josefa Drobného** propustila s tím, že o zavedení žadatelů bude informován.

8.5 Vydání certifikátů žadatelům

8.5.1 Vygenerování elektronických žádostí o certifikát

Josef Drobný dostal e-mailem zprávu, že žadatelé jsou zavedeni do systému QCA a že se mohou dostavit na kontaktní místa k vydání certifikátu.

Josef Drobný si na svém počítači vygeneroval klíčový pár a elektronickou žádost o certifikát za použití on-line generování na adrese <http://qca.postsignum.cz>. Zadal stejné údaje jako při tvorbě seznamu žadatelů. Vyplněný formulář s údaji vypadal takto:

Údaje o organizaci	
Jméno organizace:	První distribuční, a.s. *
IČ organizace:	12345678 *
Organizační jednotka:	Centrála Praha
Údaje o zaměstnanci	
Jméno a příjmení:	Josef Drobný *
Číslo zaměstnance:	254 *
E-mailová adresa:	drobny@1distribucni.cz *
Funkce zaměstnance:	technický náměstek
<input type="button" value="Smazat"/> <input type="button" value="Příklad"/>	

<input checked="" type="checkbox"/>	Povolit zálohu soukromého klíče do souboru
<input type="checkbox"/>	Změnit zabezpečení úložiště klíčů
Poskytovatel krypt. služeb:	Microsoft Enhanced Cryptographic Provider v1.0 ▼
Velikost klíče:	1024 bitů ▼
Název souboru:	C:\cert_sign.req

Po vygenerování si pro jistotu zkontroloval podle uvedených pokynů přítomnost vygenerovaných klíčů v systému a provedl jejich zálohu do souboru **zaloha_klicu.pfx**. Ten si uložil na USB disk a schoval jej do trezoru.

Elektronickou žádost o certifikát (soubor **C:\cert_sign.req**) uložil na disketu a domluvil se s kontaktním místem na termínu návštěvy.

Miroslav Táborský vygeneroval klíčový pár a žádost o certifikát v aplikaci na serveru. Žádost si rovněž uložil na disketu.

Oba se nakonec vydali na kontaktní místo s disketou s uloženou žádostí a s občanským průkazem.

8.5.2 Vydání certifikátů na kontaktním místě

Na kontaktním místě operátorka RA zkontrolovala totožnost žadatelů a zkopírovala si jejich doklady. Vytiskla písemnou žádost o certifikát, kterou žadatelé odsouhlasili svým podpisem. Následně vydala certifikát a sepsala s nimi protokol o vydání certifikátu.

8.5.3 Instalace vydaného certifikátu

Josef Drobný si v kanceláři natáhl certifikát pomocí webových stránek do systému a ve svém e-mailovém klientovi nastavil podepisování e-mailových zpráv novým klíčovým párem. Provedl export klíčů a nainstalovaného certifikátu do souboru, který uložil na USB disk, kde měl uloženou předchozí zálohu klíčů. USB disk uložil opět do trezoru. Připravil si tak zálohu klíčů pro případ havárie počítače.

Miroslav Táborský natáhl certifikát do aplikace na serveru. Firma tak začala označovat odesílané automatické odpovědi na obdržené e-mailové zprávy od obchodních partnerů. Rovněž provedl zálohu klíčů a nainstalovaného certifikátu do souboru, který přesunul na výměnné médium a to uložil na zabezpečené místo.

8.6 Dodání dalších seznamů žadatelů

Své seznamy žadatelů si připravili na pobočkách také **Arnošt Zíka** a **Iveta Vondrášová**.

Arnošt Zíka neměl v té době čas na návštěvu pracoviště ČP. Proto se dostavil s nepodepsaným úvodním listem seznamu žadatelů k notáři, kde si nechal notářsky ověřit svůj podpis. Seznam žadatelů poté nechal poslat poštou na obchodní místo Střední Čechy.

Iveta Vondrášová se dostavila osobně na kontaktní místo v Ostravě, kde se na úvodní list seznamu žadatelů podepsala před pracovníkem ČP. Kontaktní místo poté zaslalo ověřený seznam žadatelů ke zpracování na obchodní místo Střední Čechy.

Josef Drobný potřeboval po měsíci zavést do systému QCA dalšího žadatele, vedoucího nově vzniklého oddělení. Připravil proto nový seznam žadatelů. Autorita PostSignum QCA mu vydala kvalifikovaný certifikát pro ověření elektronického podpisu zaměstnanců, proto se rozhodl poslat na obchodní místo Střední Čechy elektronickou verzi seznamu žadatelů podepsaným e-mailem (podepsaným soukromým klíčem odpovídajícím vydanému certifikátu). Podepsané papírové dokumenty poslal poštou.