



Kvalifikovaná certifikační autorita

Příručka pro zákazníky – nepodnikající fyzické osoby

verze 1.0.4

Provozní dokumentace

Srpen 2007

Příručka pro zákazníky – nepodnikající fyzické osoby verze 1.0.4

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

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

1 Obsah

1 Obsah	3
2 Definice používaných pojmů	5
3 Úvod	6
3.1 Úvodní slovo.....	6
3.2 Stručně o uzavření smlouvy a vydání certifikátu.....	6
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?.....	7
4.3 Jaké certifikáty vydávané QCA budu vlastně potřebovat?.....	7
4.4 Na jakém pracovišti mohu vyřídit potřebné náležitosti?.....	8
4.5 Mám si nechat přidělit Identifikátor klienta MPSV?.....	8
4.6 Mám povolit zveřejnění certifikátu?.....	9
5 Příprava na uzavření smlouvy	9
5.1 Získání formulářů.....	9
5.2 Vyplnění objednávky.....	9
5.3 Vyplnění zákaznického formuláře.....	9
5.3.1 Zákaznický formulář Certifikáty pro ověření el. podpisu fyzické osoby.....	10
5.3.2 Zákaznický formulář Certifikáty pro ověření el. značky fyzické osoby.....	10
5.3.3 Změnový zákaznický formulář Certifikáty pro ověření el. podpisu fyzické osoby...11	
5.3.4 Změnový zákaznický formulář Certifikáty pro ověření el. značky fyzické osoby....	11
5.4 Vygenerování klíčů a elektronické žádosti o certifikát.....	12
6 Uzavření smlouvy a vydání certifikátu	12
6.1 Akceptace objednávky ze strany ČP.....	12
6.2 Vyřízení prvního zákaznického formuláře.....	12
6.3 Vydání certifikátu.....	12
6.4 Instalace vydaného certifikátu.....	13
6.5 Zneplatnění certifikátu.....	13
6.6 Doručení dalších zákaznických formulářů.....	13
6.7 Změna uzavřené smlouvy s Českou poštou.....	14
7 Ostatní	14
7.1 Fakturace.....	14
7.2 Platnost certifikátu a jeho obnova.....	14
8 Názorný příklad	15
8.1 Informace o fiktivní nepodnikající fyzické osobě.....	15
8.2 Činnosti před návštěvou kontaktního místa.....	15

8.2.1 Příprava objednávky.....	15
8.2.2 Příprava zákaznického formuláře.....	17
8.2.3 Vygenerování elektronické žádosti o certifikát.....	19
8.3 Návštěva na kontaktním místě.....	20
8.3.1 Uzavření smlouvy o poskytování certifikačních služeb.....	20
8.3.2 Vydání certifikátu.....	20
8.4 Po návštěvě na kontaktním místě.....	20
8.4.1 Instalace vydaného certifikátu.....	20

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**.

Kontaktní místo je pracoviště ČP, na němž se provádí vydávání a zneplatnění certifikátů. Také zde dochází k uzavření smlouvy s nepodnikajícími fyzickými osobami. 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.

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.

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.

Certifikační autorita **PostSignum QCA** 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 kontaktních místech.

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

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. Stáhněte si správnou verzi tohoto dokumentu.

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.

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.
- Fyzickým osobám mohou být vystaveny certifikáty podle těchto politik:
Certifikáty pro ověření elektronického podpisu fyzické osoby,
Certifikáty pro ověření elektronické značky fyzické osoby.

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. Fyzické osoby nebudou v drtivé většině případů tyto certifikáty potřebovat.
- 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 nepodnikajícím fyzickým osobám obsahují údaj „jméno a příjmení osoby“ (resp. jméno označující osoby), volitelně také údaje „adresa bydliště fyzické osoby“ a „e-mailová adresa“.
- 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 fyzické osoby je **povinná**.

4.4 Na jakém pracovišti mohu vyřídit potřebné náležitosti?

Nepodnikající fyzické osoby vyřizují veškeré náležitosti na kontaktním místě.

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 zákaznickém formuláři.

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 Příprava na uzavření smlouvy

Přestože budou fyzické osoby ve většině případů žádat pouze o vydání certifikátů pro ověření elektronického podpisu, bude v tomto postupu zmíněno také žádání o certifikát pro ověření elektronické značky.

Uzavření smlouvy spočívá v přípravě objednávky zákazníkem, která se po akceptaci na straně ČP stává smlouvou o poskytování certifikačních služeb. Fyzická osoba dále České poště předává vyplněný zákaznický formulář. Ihned po uzavření smlouvy je zákazníkovi vystaven certifikát.

5.1 Získání formulářů

Zákazník si stáhne z webových stránek QCA formulář objednávky a zákaznický formulář. 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 závodu ČP, s nímž budete uzavírat smlouvu. Pouze podle adresy zkontrolujte, zda máte staženou správnou verzi objednávky. V 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 **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 vašich osobních údajů za účelem marketingu a propagace produktů a služeb ČP. Zaškrtnutí políčka znamená, že tento souhlas neudělujete.
- Do bodu **5** doplňte vaše údaje, místo a datum.

Vyplněná objednávka se vytiskne ve dvou exemplářích. Objednávku ještě nepodepisujte.

5.3 Vyplnění zákaznického formuláře

V zákaznickém formuláři si určujete, jaké certifikáty vám budou vydány. Existují různé typy zákaznických formulářů:

- zákaznické formuláře pro vydání certifikátů podle jednotlivých certifikačních politik,

- změnové zákaznické formuláře pro správu vašich osobních údajů a vydávaných certifikátů (změna osobních údajů nebo údajů v certifikátu, vaše zablokování či vyřazení ze systému QCA, ukončení vydávání certifikátu).

Jednotlivé typy zákaznických formulářů se vyplňují následovně:

5.3.1 Zákaznický formulář Certifikáty pro ověření el. podpisu fyzické osoby

- Doplňte „Evidenční číslo smlouvy“. Tento údaj naleznete v uzavřené smlouvě, doplnilo jej kontaktní místo. Není-li smlouva ještě uzavřena, ponechte položku prázdnou.
- V první tabulce doplňte své identifikační údaje – jméno a příjmení a rodné číslo.
- V druhé tabulce doplňte povinné údaje certifikátu. Do údaje CN uveďte vaše jméno a příjmení. Jako další povinný údaj uveďte e-mailovou adresu zaměstnance.
- Stále v druhé tabulce můžete volitelně doplnit jeden nepovinný údaj – adresu vašeho bydliště.
- 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 jste zaškrtnuli, že požadujete Identifikátor klienta MPSV, musíte vyplnit druhou stránku formuláře. Zde se nachází formulář, v němž udělujete souhlas s poskytnutím osobních údajů pro MPSV. Vyplnění a podepsání formuláře je podmínkou pro přidělení identifikátoru MPSV.

Vytiskněte zákaznický formulář, ale ještě jej nepodepisujte. Formulář pro MPSV se musí vytisknout na samostatný papír, nepoužívejte proto oboustranný tisk.

5.3.2 Zákaznický formulář Certifikáty pro ověření el. značky fyzické osoby

- Doplňte „Evidenční číslo smlouvy“. Tento údaj naleznete v uzavřené smlouvě, doplnilo jej kontaktní místo. Není-li smlouva ještě uzavřena, ponechte položku prázdnou.
- V první tabulce doplňte své identifikační údaje – jméno a příjmení a rodné číslo.
- V druhé tabulce doplňte povinný údaj certifikátu CN – uveďte sem jméno certifikátu pro označující zařízení.
- Stále v druhé tabulce můžete volitelně doplnit nepovinné údaje – adresu vašeho bydliště a e-mailovou adresu. 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).

Vytiskněte zákaznický formulář, ale ještě jej nepodepisujte.

Pokud jméno certifikátu obsahuje tzv. doménové jméno (např. **epost.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 QCA. (Předpokládáme však, že fyzické osoby většinou nebudou požadovat vydání kvalifikovaných systémových certifikátů s doménovými jmény.)

5.3.3 Změnový zákaznický formulář Certifikáty pro ověření el. podpisu fyzické osoby

- Doplňte „Evidenční číslo smlouvy“. Tento údaj naleznete v uzavřené smlouvě, doplnilo jej kontaktní místo. Není-li smlouva ještě uzavřena, ponechte položku prázdnou.
- V první tabulce doplňte své identifikační údaje – jméno a příjmení a rodné číslo.
- V druhé tabulce doplňte stávající znění povinných a nepovinných údajů příslušného certifikátu.
- V části Správa údajů o zákazníkovi máte možnost změnit své osobní údaje, zablokovat, odblokovat nebo se zcela vyřadit 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. Pokud požadujete vložení Identifikátoru klienta MPSV do certifikátu, je potřeba vyplnit třetí stránku formuláře. Zde se nachází formulář, v němž udělujete souhlas s poskytnutím osobních údajů pro MPSV. Vyplnění a podepsání formuláře je podmínkou pro přidělení identifikátoru MPSV.

Vytiskněte zákaznický formulář, ale ještě jej nepodepisujte.

5.3.4 Změnový zákaznický formulář Certifikáty pro ověření el. značky fyzické osoby

- Doplňte „Evidenční číslo smlouvy“. Tento údaj naleznete v uzavřené smlouvě, doplnilo jej kontaktní místo. Není-li smlouva ještě uzavřena, ponechte položku prázdnou.
- V první tabulce doplňte své identifikační údaje – jméno a příjmení a rodné číslo.
- V druhé tabulce doplňte stávající znění povinných a nepovinných údajů příslušného certifikátu.
- V části Správa údajů o zákazníkovi máte možnost změnit své osobní údaje, zablokovat, odblokovat nebo se zcela vyřadit ze systému QCA.
- V části Správa údajů o certifikátu máte možnost změnit údaje certifikátu, změnit zveřejnění certifikátu nebo zcela zrušit vydávání certifikátu.

Vytiskněte zákaznický formulář, ale ještě jej nepodepisujte.

Pokud dochází ke změně jména certifikátu a jméno po změně obsahuje tzv. doménové jméno (např. **epost.cz** nebo **mojedomena.com**), musíte připojit ke změnovému zákaznickému formuláři prohlášení vlastníka domény, v němž stvrzujete, že vlastníte danou doménu. Formulář lze stáhnout z webových stránek QCA. (Předpokládáme však, že fyzické osoby většinou nebudou požadovat vydání kvalifikovaných systémových certifikátů s doménovými jmény.)

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 QCA nabízeny příslušné nástroje. Na webových stránkách si dále můžete stáhnout příručky popisující postupy generování klíčů v těchto nástrojích.

6 Uzavření smlouvy a vydání certifikátu

Dostavíte se na kontaktní místo s:

- vyplněnou objednávkou,
- zákaznickým formulářem,
- 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 RA podepíšete oba exempláře objednávky.

6.1 Akceptace objednávky ze strany ČP

Operátor RA ověří vaši identitu podle obou dokladů totožnosti. Zkopíruje osobní doklady z důvodu následného vydávání certifikátu, což stanovuje zákon č.227/2000 Sb. o elektronickém podpisu.

Operátor RA zkontroluje údaje v objednávce a v případě správnosti ji akceptuje. Od operátora obdržíte jeden exemplář podepsané objednávky.

6.2 Vyřízení prvního zákaznického formuláře

Před operátorem RA se podepíšete na zákaznický formulář(e).

Kontaktní místo vás na základě zákaznického formuláře zavede do systému QCA. Poté se může přistoupit k vydání certifikátu.

6.3 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 6.5). Toto heslo určujete vy. Není nutné si je pamatovat, protože bude uvedeno v protokolu o vydání certifikátu. Heslo by se nemělo shodovat s jinými hesly, která běžně používáte.

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

Máte 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. Musíte si vygenerovat nový klíčový pár a žádost o certifikát a navštívit kontaktní místo znovu.

6.4 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.

6.5 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.

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

Operátorce dále sdělíte heslo pro zneplatnění, které je opět uvedeno v protokolu o vydání certifikátu. Tímto se ověří, zda-li máte oprávnění žádat o zneplatnění daného certifikátu. Pokud heslo nesouhlasí, nebo je neznáte, musíte se na kontaktní místo dostavit osobně (se dvěma doklady totožnosti) a vyplnit písemnou žádost o zneplatnění certifikátu (vzor žádosti lze stáhnout z webových stránek QCA). Certifikát je zneplatněn po ověření dokladů. Doklady jsou opět zkopírovány, stejně jako při vydávání certifikátu.

Na konci procesu obdržíte 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 vám doporučí návštěvu kontaktního místa během pracovní doby.

6.6 Doručení dalších zákaznických formulářů

Příprava dalších zákaznických formulářů může být potřeba z těchto důvodů:

- chcete si nechat vydat další certifikáty s jinými údaji
- požadujete změnu údajů ve stávajících vydaných certifikátech nebo ukončit jejich vydávání
- došlo ke změně vašich osobních údajů
- chcete se nechat vyřadit ze systému QCA

Vyplněný zákaznický formulář(e) doručíte osobně na kontaktní místo osobně a podepíšete se před pracovníkem ČP.

Operátor RA zanese údaje ze zákaznického formuláře do systému QCA. Poté může dojít k vydání nového certifikátu nebo certifikátu se změněnými údaji.

6.7 Změna uzavřené smlouvy s Českou poštou

V případě změny vašich osobních údajů nebo jiných ustanovení ve smlouvě je uzavřen dodatek ke smlouvě s obchodním místem v daném regionu. Další detaily uzavření dodatku jsou dohodnuty s obchodním místem (např. zaslání dodatku poštou nebo podepsání dodatku na kontaktním místě).

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. Vydaný certifikát je zaplacen v hotovosti na kontaktním místě. Doklad o zaplacení je součástí protokolu o vydání certifikátu.

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, je možné opět si nechat vystavit nový certifikát osobně na kontaktním místě – provedou se postupy popsané v kapitolách 5.4, 6.3 a 6.4.

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

Pokud došlo ke změnám, doručíte na kontaktní místo „změnové“ zákaznické formuláře. Kontaktní místo provede příslušné změny v systému QCA a informuje vás o provedení změn. Poté se můžete dostavit na kontaktní místo nechat si vydat nový certifikát.

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

8 Názorný příklad

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

8.1 Informace o fiktivní nepodnikající fyzické osobě

Paní **Kateřina Nováková** je moderní žena, která chce komunikovat elektronickou cestou s úřady státní správy. Proto hodlá využít služeb QCA a nechat si vydat kvalifikovaný certifikát.

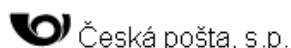
8.2 Činnosti před návštěvou kontaktního místa

8.2.1 Příprava objednávky

Kateřina Nováková si stáhla z adresy <http://qca.postsignum.cz> vzor objednávky pro fyzické osoby. Po prostudování dokumentu se rozhodla, že:

- smlouvu uzavře na dobu neurčitou,
- objedná služby vydání certifikátů kvalifikovanou i komerční autoritou (v budoucnu se to může hodit),
- neposkytne souhlas s používáním osobních údajů pro marketingové účely ČP.

Vyplněná objednávka vypadala následovně:



Česká pošta, s.p.

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 Jižní Morava

se sídlem Orlí 655/30, 663 00 Brno

IČ: 47114983

DIČ: CZ47114983

zapsaná v obchodním rejstříku, vedeném u Krajského soudu v Brně, sp.zn. A 5092

Bankovní spojení ČSOB, a.s., č.ú.133406370/0300

Zákazník

Jméno a příjmení **Kateřina Nováková**

Bydliště **Dvořákova 4, 602 00 Brno**

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 fyzické osoby (kvalifikovaný certifikát)
- certifikát určený k ověření elektronické značky fyzické osoby (kvalifikovaný systémový certifikát)

Certifikáty vydávané komerční certifikační autoritou PostSignum: →

- certifikát fyzických osob (komerční certifikát)
- certifikát technologických komponent 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 Reklamací poskytovaných služeb se provádí výhradně v místě poskytnutí služby. Poskytovatel sepíše se zákazníkem reklamační protokol. V případě oprávněné reklamací bude sjednána náprava nejpozději do 14 dnů od sepsání reklamačního protokolu. V případě neoprávněné reklamací bude zákazník poskytovatelem informován o důvodu neuznání reklamací.

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

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

4.8 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

Za zákazníka

Brno 4.9.2006
..... Místo Datum

Kateřina Nováková
..... Jméno a příjmení Podpis

Objednávku pak vytiskla ve dvou exemplářích, ještě ji nepodepisovala.


8.2.2 Příprava zákaznického formuláře

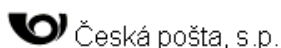
Kateřina Nováková si z adresy <http://qca.postsignum.cz> stáhla standardní zákaznický formulář „Certifikáty pro ověření elektronického podpisu fyzické osoby“.

V záhlaví formuláře ponechala prázdné evidenční číslo smlouvy, protože to není ještě přiděleno. V první tabulce vyplnila své jméno a příjmení a rodné číslo.

V druhé tabulce zadala do pole CN své jméno a příjmení a doplnila svoji e-mailovou adresu. Do nepovinného údaje L zadala svoji adresu ve tvaru „město ulice číslo“.

Dále povolila zveřejnění svého certifikátu, aby si jej mohli stáhnout komunikující partneři. Také požádala o uvedení „identifikátoru klienta MPSV“ v certifikátu. Vyplnila souhlas pro MPSV na druhé stránce. Zákaznický formulář vypadal po vyplnění takto:

 Česká pošta, s.p.		PostSignum QCA
Údaje pro vydání certifikátu určeného k ověření elektronického podpisu fyzické osoby (kvalifikovaný certifikát)		
Evidenční číslo smlouvy (objednávky): 		
Údaje o zákazníkovi		
Jméno a příjmení	Kateřina Nováková	
Rodné číslo (pro občany ČR)	888888/9999	
Datum narození, číslo a typ dokladu (pro cizince)		
Údaje o certifikátu		
Povinné položky		
CN (jméno a příjmení, tituly) <i>(max. 100 znaků)</i>	Kateřina Nováková	
Adresa elektronické pošty <i>(max. 250 znaků)</i>	knovakova@email.cz	
Nepovinné položky		
L (adresa bydliště)* <i>(max. 100 znaků)</i>	Brno Dvořákova 4	
<p><i>V případě rozporu údajů CN a L s údaji v předložených dokladech se do certifikátu vloží údaje z dokladů.</i></p> <p>* <i>Vyplňte pouze v případě, že chcete mít adresu bydliště uvedenou v certifikátu.</i></p>		
<p>V případě, že si nepřejete zveřejnění vydaného certifikátu nebo vydaných certifikátů na webových stránkách (adresářových službách) České pošty, zaškrtněte <input type="checkbox"/></p> <p>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.</p> <p>Pokud si přejete, aby váš kvalifikovaný certifikát obsahoval identifikátor klienta Ministerstva práce a sociálních věcí, zaškrtněte <input checked="" type="checkbox"/></p>		
<p>Zákazník 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.).</p> <p>Zákazník 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. Zákazník bere na vědomí, že pokud tyto informace neuvede, nemůže mu být ze strany České pošty poskytnuta požadovaná služba.</p> <p>Zákazník dále bere na vědomí informace o svém právu na přístup k osobním údajům, které jsou zpracovány za účelem poskytnutí jím požadované služby, právu na opravu těchto osobních údajů i povinnosti České pošty na požádání zákazníkovi sdělit informace o jejich zpracování, jakož i o dalších právech stanovených v §21 zákona č. 101/2000 Sb.</p>		
<p>Zaškrtnutím okénka, aby váš kvalifikovaný certifikát obsahoval identifikátor klienta Ministerstva práce a sociálních věcí, se na vás vztahují následující zvláštní ustanovení:</p> <ul style="list-style-type: none"> • Zákazník 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 poživateli těchto dávek a žadatelích o tyto dávky (dále jen „klient MPSV“) a osobách s nimi společně posuzovaných (dále jen „informační systém MPSV“). • Zákazník - 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 zákazníka – klienta MPSV v informačním systému MPSV při elektronické komunikaci zákazníka – klienta MPSV a MPSV. • Zákazník - klient MPSV nebo budoucí klient MPSV svým podpisem přílohy č.2 této smlouvy 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 zákazníků – klientů MPSV nebo budoucích klientů MPSV, kterým byl Českou poštou vydán kvalifikovaný certifikát. Evidence je vedena výhradně pro účely prokázání totožnosti zákazníka – klienta MPSV v případě jeho elektronické komunikace s MPSV podle zákona o státní sociální podpoře. Evidence obsahuje tyto údaje: jméno a příjmení zákazníka, rodné číslo nebo ekvivalentní údaj, ze kterého je zřejmé pohlaví žadatele, titul před jménem a za příjmením žadatele, a adresu pobytu zákazníka. 		
..... Podpis zákazníka		
Zákaznické formuláře: zákazník – fyzická osoba		



PostSignum QCA

Souhlas zákazníka 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:

Zákazník souhlasí s tím, že MPSV bude pro účely prokázání totožnosti zákazníka – 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 zákazníka, rodné číslo nebo ekvivalentní údaj, ze kterého je zřejmé pohlaví zákazníka, titul před jménem a za příjmením zákazníka a adresu pobytu zákazníka. Souhlas se uděluje na dobu neurčitou.

V Brně dne 4.9.2006

Zákazník:

Jméno: Kateřina

Příjmení: Nováková

Datum narození: 17.7.1980

Adresa pobytu:

Obec - město: Brno

Část obce:

Ulice: Dvořákova

Číslo: 4

PSČ: 602 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.

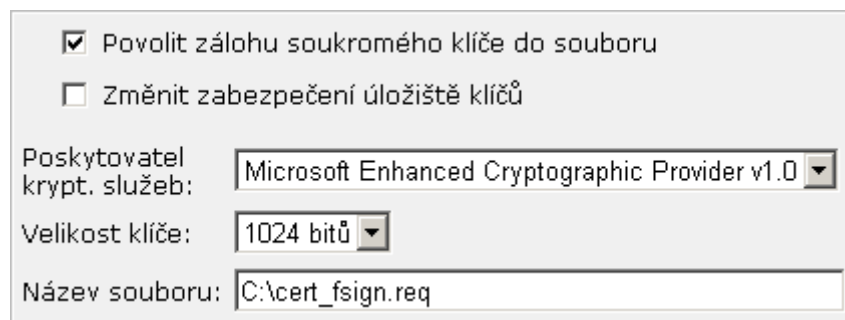
Zákaznické formuláře: zákazník – fyzická osoba

Zákaznický formulář vytiskla, ale ještě nepodepisovala.

8.2.3 Vygenerování elektronické žádosti o certifikát

Kateřina Nováková si na svém počítači vygenerovala klíčový pár a elektronickou žádost o certifikát. Využila přitom webové stránky na adrese <http://qca.postsignum.cz> a zadala stejné údaje jako při tvorbě zákaznického formuláře. Vyplněný formulář na webové stránce vypadal takto:

Jméno a příjmení:	<input type="text" value="Kateřina Nováková"/>	*
E-mailová adresa:	<input type="text" value="knovakova@email.cz"/>	*
Ulice a číslo domu:	<input type="text" value="Dvořákova 4"/>	
Město:	<input type="text" value="Brno"/>	
<input type="button" value="Smazat"/> <input type="button" value="Příklad"/>		



Po vygenerování si pro jistotu zkontrolovala podle uvedených pokynů přítomnost vygenerovaných klíčů v systému a provedla jejich zálohu do souboru **zaloha_klicu.pfx**. Ten si uložila na USB disk a schovala jej na bezpečné místo.

Elektronickou žádost o certifikát (soubor **C:\cert_sign.req**) uložila na disketu, kterou si vezme na kontaktní místo.

8.3 Návštěva na kontaktním místě

8.3.1 Uzavření smlouvy o poskytování certifikačních služeb

Kateřina Nováková si s kontaktním místem domluvila termín návštěvy a s sebou přinesla vyplněné objednávky, zákaznický formulář a dva své doklady totožnosti (občanský a řidičský průkaz). Zároveň přinesla disketu s elektronickou žádostí o certifikát.

Operátorka ověřila její identitu vůči předloženým dokladům, které si zkopírovala. Před operátorkou kontaktního místa **Kateřina Nováková** podepsala zákaznický formulář. Operátorka akceptovala objednávku a uzavřela tak smlouvu. Podepsanou akceptací objednávky předala **Kateřině Novákové**.

Operátorka RA zavedla **Kateřinu Novákovou** do systému QCA. Nakonec operátorka RA provedla vydání certifikátu.

8.3.2 Vydání certifikátu

Operátorka RA připravila na základě elektronické žádosti písemnou žádost o certifikát, kterou vytiskla. **Kateřina Nováková** žádost schválila svým podpisem. Operátorka RA vydala certifikát a sepsala s ní protokol o vydání certifikátu.

8.4 Po návštěvě na kontaktním místě

8.4.1 Instalace vydaného certifikátu

Doma si **Kateřina Nováková** natáhla prostřednictvím webových stránek certifikát do systému a ve svém e-mailovém klientovi nastavila podepisování e-mailových zpráv novým klíčovým párem.

Dále provedla export klíčů a nainstalovaného certifikátu do souboru, který uložila na USB disk, kde měla uloženou předchozí zálohu klíčů. USB disk uložila opět na bezpečné místo. Připravila si tak zálohu klíčů pro případ havárie počítače.