Česká pošta

# Příručka pro zákazníky – nepodnikající fyzické osoby

Verze 3.0

| | | | |
|---|---|---|---|
| **Podpis** | podepsáno elektronicky | **Podpis** | podepsáno elektronicky |
| **Datum** | 21. 7. 2014 | **Datum** | 21. 7. 2014 |
| **Garant dokumentu** | Ing. Miroslav Trávníček | **Schvalovatel** | Ing. Pavel Plachý |
| **Funkce** | Vedoucí odd. vývoje QCA/VCA | **Funkce** | Ředitel odboru PKNU |

# Obsah dokumentu

**1. Definice používaných pojmů ..... 4**
**2. Úvod ..... 5**
2.1. Úvodní slovo ..... 5
2.2. Stručně o uzavření smlouvy a vydání prvotního certifikátu ..... 5
2.3. Zdroje informací o CA ..... 5
**3. Než dojde k uzavření smlouvy… ..... 6**
3.1. Mám požádat o kvalifikovaný nebo komerční certifikát? ..... 6
3.2. Mám certifikační služby využívat jako zástupce/zaměstnanec organizace, OSVČ či nepodnikající fyzická osoba? ..... 6
3.3. Jaké certifikáty vydávané CA budu vlastně potřebovat? ..... 6
3.4. Na jakém pracovišti mohu vyřídit potřebné náležitosti? ..... 7
3.5. Mám si nechat přidělit Identifikátor klienta MPSV? ..... 7
3.6. Mám povolit zveřejnění certifikátu? ..... 7
**4. Uzavření smlouvy ..... 7**
4.1. Získání formulářů ..... 7
4.2. Vyplnění smlouvy ..... 8
4.2.1. Změna uzavřené smlouvy s Českou poštou ..... 8
4.3. Vyplnění formuláře Údaje pro vydání certifikátu ..... 8
4.3.1. Změna údajů pro vydání certifikátu ..... 8
4.4. Vygenerování klíčů a elektronické žádosti o certifikát ..... 9
**5. Vydání certifikátu ..... 9**
5.1. Instalace vydaného certifikátu ..... 10
5.2. Zneplatnění certifikátu ..... 10
**6. Ostatní ..... 10**
6.1. Fakturace ..... 10
6.2. Platnost certifikátu a jeho obnova ..... 10

# Evidence revizí a změn

| Verze | Účinnost od | Důvod a popis změny | Autor | Schválil |
|---|---|---|---|---|
| 0.1 | 14.1.2006 | První verze | M.Šlancar | Manažer QCA |
| 1.01 | 19.1.2006 | Opravena chyba v kapitole 4.1 | M.Šlancar | Manažer QCA |
| 1.03 | 23.9.2006 | Aktualizovány postupy a obrázky na základě změny webových stránek a zákaznických formulářů | M.Šlancar | Manažer QCA |
| 1.0.4 | 18.8.2007 | Aktualizován seznam osobních dokladů v kapitole 6 | M.Šlancar | Manažer QCA |
| 2.0 | 6.9.2010 | Aktualizovány postupy na základě nových formulářů a webových stránek | Petr Huptich | Manažer CA |
| 2.1 | 1.8.2012 | Aktualizace dokumentu | H. Radová Švecová | Manažer CA |
| 3.0 | 21. 7. 2014 | Aktualizace dokumentu | M. Haubeltová | Manažer CA |

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

# 1. Definice používaných pojmů

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

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

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

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

**Pobočka České pošty se službou Czech POINT** je pracoviště ČP, na němž se provádí uzavírání smluv, vydávání certifikátů a zneplatnění certifikátů. **Zákazníkem** je myšlena fyzická osoba (jednotlivec), podnikající fyzická osoba (OSVČ) či právnická osoba (organizace), která vstoupila do smluvního vztahu s ČP s tím, že s ní byla uzavřena *Smlouva o poskytování certifikačních služeb* ČP.

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

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

**MPSV** je zkratka Ministerstva práce a sociálních věcí.

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

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

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

**Elektronická žádost o certifikát (zpravidla soubor s příponou req)** je datová struktura, pomocí níž lze žádat o certifikát. V žádosti je uložen veřejný klíč, který se „přenese" do vydaného certifikátu.

**Certifikát** představuje datovou strukturu, která je svázána s určitou osobou. Pomocí certifikátu lze tedy tuto osobu jednoznačně identifikovat. Pomocí certifikátu lze ověřit elektronický podpis dané osoby. Součástí vydaného certifikátu jsou informace o držiteli certifikátu, doba platnosti, účel použití, veřejný klíč a případně další informace. Obsah certifikátu je podepsán vydávající certifikační autoritou, aby bylo možné prokázat, že byl touto autoritou skutečně vydán.

**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 C**ertificate Revocation List**, a především z něj odvozená zkratka **CRL**.

# 2. Úvod

## 2.1. Úvodní slovo

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

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

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

## 2.2. Stručně o uzavření smlouvy a vydání prvotního certifikátu

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

Navržené postupy předpokládají okamžité vydání certifikátu po uzavření smlouvy. Nepodnikající fyzické osoby jsou kompletně odbavovány na pobočkách České pošty se službou Czech POINT. V následujících kapitolách si detailněji popíšeme celý proces od přípravy objednávky a zákaznického formuláře přes uzavření smlouvy až po finální vydání certifikátu žadateli.

## 2.3. Zdroje informací o CA

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

# 3. Než dojde k uzavření smlouvy…

## 3.1. Mám požádat o kvalifikovaný nebo komerční certifikát?

**Kvalifikované certifikáty** lze použít při komunikaci s orgány státní správy. 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.

**Komerční certifikáty** mohou být použity nejen za účelem podepisování dat, ale také pro jejich zašifrování a k autentizaci do různých systémů, například k systému ISDS. Nejsou akceptovány při komunikaci se státní správou. Pokud však chcete používat certifikáty pro zajištění šifrování dat, nevyhnete se pořízení komerčního certifikátu.

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

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

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

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

## 3.3. Jaké certifikáty vydávané CA budu vlastně potřebovat?

Každá certifikační autorita obecně nabízí poměrně specializované služby. Zákazník by se měl předem rozhodnout, jaký typ certifikátu bude potřebovat. Příslušné informace o vydávaných certifikátech jsou uvedeny v certifikačních politikách - ty naleznete na webových stránkách www.postsignum.cz. V této kapitole se pokusíme vyjmenovat ty nejdůležitější body, které by vám měly pomoci při výběru správného typu certifikátu pro vás. Dále uvedeme důležité informace související s vydáváním certifikátů.

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

  **Kvalifikované osobní certifikáty**

  **Komerční osobní certifikáty**

  **Kvalifikované systémové certifikáty**

  **Komerční serverové certifikáty**

Osobní certifikáty kvalifikované i komerční a jsou určeny pro osoby. Certifikáty vydané podle ostatních politik jsou určeny pro technická zařízení (např. aplikace na serverech).

- Kvalifikované osobní certifikáty použijete zejména pro komunikaci se státní správou. Pokud chcete komunikovat s úřady státní správy, chtějte, aby byl v certifikátu obsažen „Identifikátor klienta MPSV“.
- O Kvalifikované systémové certifikáty budou žádat nejčastěji právě orgány státní správy, které hodlají provozovat tzv. elektronické podatelny. Fyzické osoby nebudou v drtivé většině případů tyto certifikáty potřebovat.
- Pro šifrování dat a autentizaci jsou určeny certifikáty vydávané autoritou PostSignum VCA – komerční certifikáty.
- Komerční certifikáty nejsou uznávány při komunikaci s úřady státní správy. Pro komunikaci se státní správou použijte kvalifikované certifikáty.

### 3.4. Na jakém pracovišti mohu vyřídit potřebné náležitosti?

Nepodnikající fyzické osoby vyřizují veškeré náležitosti na pobočce České pošty se službou Czech POINT, nebo na obchodním místě CA. Certifikáty lze také získat na Externí registrační autoritě.

### 3.5. 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 ani 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.

### 3.6. Mám povolit zveřejnění certifikátu?

Zveřejnění či nezveřejnění certifikátu se nastavuje v údajích pro vydání certifikátu.

Zveřejnění certifikátu znamená, že veřejná část certifikátu bude přístupná uživatelům, kteří si jej pak mohou stáhnout z webových stránek PostSignum CA např. z důvodu ověření, že takový certifikát existuje, apod.

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

## 4. Uzavření smlouvy

Uzavření smlouvy spočívá v přípravě formuláře smlouvy zákazníkem a jejím potvrzení na pracovišti České pošty. Fyzická osoba dále České poště předává vyplněný formulář *Údaje pro vydání certifikátu*.

### 4.1. Získání formulářů

Zákazník si stáhne z webových stránek CA formulář smlouvy a formulář *Údaje pro vydání certifikátu*.

## 4.2. Vyplnění smlouvy

Formulář vyplňte podle těchto pokynů:

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

Vyplněný formulář smlouvy se vytiskne ve dvou exemplářích.

### 4.2.1. Změna uzavřené smlouvy s Českou poštou

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

## 4.3. Vyplnění formuláře Údaje pro vydání certifikátu

Ve formuláři si určujete, jaký druh certifikátu vám bude vystaven.

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

### 4.3.1. Změna údajů pro vydání certifikátu

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

Pokud má zákazník osobní certifikát vydaný certifikační autoritou České pošty PostSignum, může tento formulář včetně příloh poslat **elektronicky podepsaným e-mailem** na obchodní místo certifikační autority České pošty. Seznam obchodních míst, včetně kontaktů, naleznete na webových stránkách www.postsignum.cz.

Po obdržení formuláře operátor zanese údaje do systému CA. O provedené změně budete informováni, k vydání nového certifikátu může dojít až po provedené změně.

### 4.4. Vygenerování klíčů a elektronické žádosti o certifikát

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

Po vygenerování klíčů je povinností žadatele provést zálohu vygenerovaného soukromého klíče. Návod na provedení zálohy klíče při vygenerování žádosti prostřednictvím webových stránek, je uvedena na webových stránkách PostSignum.

## 5. Vydání certifikátu

- Pro vydání prvotního certifikátu se musí žadatel o certifikát dostavit osobně na pobočku ČP se službou Czech POINT. Je nutné se dostavit s vyplněným formulářem smlouvy (dvojí vyhotovení),
- s formulářem Údaje pro vydání certifikátu
- **se dvěma osobními doklady totožnosti** (občanský průkaz, cestovní pas, řidičský průkaz, průkaz ZTP nebo rodný list – povinně musí být vždy předložen první nebo druhý uvedený doklad).
- **ID vygenerované žádosti o certifikát** uložené na www serveru, případně se žádostí (ve formátu PKCS#10 – většinou má soubor příponu REQ) uloženou na USB flash disku

*Poznámka*: Pokud vlastníte slevovou poukázku certifikační autority a chcete ji uplatnit, předložte ji na přepážce při vydání certifikátu.

Po předložení všech potřebných dokumentů a překontrolování údajů přejde pracovník k samotnému vydání certifikátu. V průběhu vydávání certifikátů pracovník vytiskne *Žádost o vydání certifikátu,* kterou předloží žadateli ke kontrole a k podpisu. Žadatel tak svým podpisem schválí správnost údajů ve vydaném certifikátu.

Na žádosti se uvádí tzv. *Heslo pro zneplatnění*, které souvisí s procesem zneplatnění certifikátu (viz kapitola 5.2). Toto heslo se ve většině případů generuje automaticky, můžete si ale také zažádat o heslo vlastní. Není nutné si jej pamatovat, protože bude uvedeno v *Protokolu o vydání certifikátu*. Heslo by se nemělo shodovat s jinými hesly, která běžně používáte.

Vydaný certifikát lze přijmout:

- osobně podepsáním *Protokolu o vydání certifikátu*. V tomto případě může být certifikát uložen na přenosné médium zákazníka
- potvrzením přijetí přes www stránky PostSignum na základě doručeného e-mailu, který obsahuje odkaz na webovou stránku s *Protokolem o vydání certifikátu*

Žadatel má také právo vydaný certifikát odmítnout. V případě nepřijetí certifikátu je certifikát automaticky zneplatněn. V případě odmítnutí na pobočce je navíc vytištěn *Protokol o nevydání certifikátu.* **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 pobočku znovu.

### 5.1. Instalace vydaného certifikátu

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

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

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

Po instalaci certifikátu doporučujeme provést zálohu certifikátu včetně privátního klíče pro případ obnovy certifikátu a klíčů např. po havárii počítače, apod. Návod na provedení zálohy certifikátu v OS Windows naleznete na webových stránkách PostSignum.

Spolu s vydaným certifikátem je potřeba nainstalovat do cílové aplikace také certifikáty certifikačních autorit PostSignum.

*Poznámka:* Od 24. 5. 2010 jsou certifikáty autorit PostSignum v programu Microsoft Root. Ve všech verzích Windows budou tedy certifikáty PostSignum důvěryhodné.

### 5.2. Zneplatnění certifikátu

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

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

## 6. Ostatní

### 6.1. Fakturace

Ceník služeb CA je k dispozici na webových stránkách CA.

Vydaný certifikát je zaplacen v hotovosti na pobočce České pošty se službou Czech POINT. Případně můžete předložit při vydání zakoupenou certifikační poukázku. V tom případě se cena v hotovosti nehradí.

Za vydání následného certifikátu (prostřednictvím elektronické Podatelny PostSignum), platíte předem poukázáním příslušné částky na účet České pošty. Informace o platbě jsou zasílány e-mailem.

### 6.2. Platnost certifikátu a jeho obnova

**Platnost vydaného certifikátu je 365 dní (1 rok), po uplynutí platnosti certifikátu nedochází k automatické obnově.** Certifikační autorita PostSignum nabízí možnost vydání následného certifikátu, který je taktéž zpoplatněn. **Platnost následného certifikátu vydaného elektronicky je prodloužena o 20 dní na 385 dní**.

Následný certifikát lze vystavit:

- osobní návštěvou pobočky České pošty se službou Czech POINT nebo obchodního místa
- elektronicky pomocí webové aplikace
- pomocí elektronicky podepsaného e-mailu odeslaného na podatelnu PostSignum

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

Pokud došlo ke změnám, které chcete promítnout do certifikátu, doručíte na pobočku České pošty se službou Czech POINT změnu údajů pro vydání certifikátu (viz.bod 4.3.1). V systému CA dojde k provedení příslušné změny a následně budete o provedení změny informováni. Poté si můžete nechat vystavit nový certifikát.

**Pozor!** Pokud dojde ke změně jména nebo příjmení, případně titulů, bude nutné si pro certifikát zajít opět na pobočku ČP, viz vydání prvotního certifikátu.