**Univerzita Pardubice**
**Fakulta ekonomicko-správní**

# Využití elektronického podpisu ve vybraných orgánech státní správy a možnosti jeho dalšího uplatnění

**Olga Raková**

**Bakalářská práce**
**2008**

**Univerzita Pardubice**
**Fakulta ekonomicko-správní**
**Ústav systémového inženýrství a informatiky**
Akademický rok: **2007/2008**

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Olga MARKOVÁ**

Studijní program: **B6209 Systémové inženýrství a informatika**

Studijní obor: **Regionální a informační management**

Název tématu: **Využití elektronického podpisu ve vybraných orgánech státní správy a možnosti jeho dalšího uplatnění**

Zásady pro vypracování:

1. Vysvětlení pojmu – elektronický podpis
2. Právní úprava
3. Certifikační autority – stručné srovnání nabízených služeb
4. Výběr orgánů státní správy
5. Hodnocení současného stavu využití elektrického podpisu
6. Návrh možností dalšího uplatnění

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:


**[1] HANÁČEK, Petr, STAUDEK, Jan. Bezpečnost informačních systémů: Metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií. 1. vyd. Praha: Úřad pro státní informační systém, 2000. 130 s. ISBN 80-238-5400-3.**

**[2] Státní informační a komunikační politika. Ministerstvo informatiky České republiky, 2005.**

**[3] Platná legislativa.**


Vedoucí bakalářské práce: **Ing. Tomáš Kořínek**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **1. října 2007**

Termín odevzdání bakalářské práce: **19. května 2008**

prof. Ing. Jan Čapek, CSc.
děkan

L.S.

doc. Ing. Pavel Petr, Ph.D.
vedoucí ústavu

V Pardubicích dne 31. října 2007

SOUHRN

Práce popisuje využívání elektronického podpisu při komunikaci občanů a organizací se státní správou. Zabývá se legislativou a jejím vývojem. Srovnává služby, které jsou nabízeny kvalifikovanými certifikačními autoritami. Mapuje možnosti pro elektronická podání v organizacích státní správy. Zaměřuje se na zhodnocení současného stavu u vybraných orgánů státní správy, výhod a nevýhod elektronických podání a možností dalšího využití.

KLÍČOVÁ SLOVA

zaručený elektronický podpis, kvalifikovaný certifikát, kvalifikovaný systémový certifikát, elektronická podatelna, kvalifikovaný poskytovatel certifikačních služeb

TITLE

Utilization of an electronic signature in selected authorities of civil service and possibilities o its further use

ABSTRACT

This work describes the use of electronic signature in the communication of citizens and the state administration. It deals with legislation and its development. Scores services that are offered to qualified certification authorities. It maps options for electronic filing in government organizations. It focuses on the assessment of the status quo for selected government, the advantages and disadvantages of electronic filing and the possibility of further use.

KEYWORDS

advanced electronic signature, qualified certificate, qualified systems testimonia, electronic registry, qualified provider of testimonial services

# OBSAH

# Úvod

Internet stále více vstupuje do našeho každodenního života. Zároveň s tímto rychlým nástupem vznikají také mnohá úskalí, která je nutné překonat. Jedním z nich je přiblížení internetu co nejširším vrstvám obyvatelstva a druhým je dosáhnout co nejvyšší míry informační gramotnosti ve společnosti, která by výhody informačních a komunikačních technologií mohla co nejlépe využít ve svůj prospěch.

Tato úskalí nezůstala lhostejná ani Vládě České republiky. Jednou z oblastí, na kterou se zaměřila, je oblast e-governmentu. Hlavním cílem je zvýšit výkonnost státní správy a tak zjednodušit styk občanů s veřejnou správou. S tímto je i úzce spojená problematika elektronického podpisu, který by měl po vhodných úpravách legislativy usnadnit komunikaci občanů se státní správou prostřednictvím internetu.

Cílem práce je podat přehled o tom, se kterými orgány státní správy lze elektronicky komunikovat za využití zaručeného elektronického podpisu a zhodnocení současného stavu jeho využívání. V první kapitole jsou vysvětleny klíčové pojmy bezprostředně související s elektronickým podpisem, ukázána cesta od výběru kvalifikované certifikační autority až po získání kvalifikovaného elektronického podpisu založeném na kvalifikovaném certifikátu, který je jako jediný akceptován státní správou. Závěr kapitoly je věnován symetrickému a asymetrického šifrování na jehož principech elektronický podpis funguje. Druhá kapitola se zabývá legislativou a je zde uveden přehled vývoje právních norem a zákonů. Ve třetí kapitole jsou uvedeny kvalifikované certifikační autority, tedy kvalifikovaní poskytovatelé certikačních služeb, shrnuty služby, které jednotlivé autority nabízejí a je provedeno porovnání těchto služeb podle zvolených kritérií. Dále je ukázán vývoj vydávání kvalifikovaných certifikátů jednotlivými autoritami a vzájemné porovnání tohoto vývoje v době, kdy již všechny tři autority působily na trhu společně. Následující čtvrtá kapitola mapuje možnosti elektronických podání u orgánů státní správy, tedy které datové zprávy je nutné opatřit zaručeným elektronickým podpisem a které nikoli, jaké jsou postupy při elektronických podáních a které orgány státní správy jsou největšími příjemci elektronických podání. V páté kapitole je popsán současný stav u vybraných orgánů státní správy, podle předem zvolených kritérií. První tři kriteria jsou společná pro všechny vybrané orgány státní správy a zaměřuji se zde na to, jaké jsou možnosti učinit e-podání, zda je potřeba specielní software a jaký je vývoj e-podání v jednotlivých letech. Další kritéria jsou již volena individuelně podle posuzovaných oblastí.

# 1. Základní pojmy

V této kapitole jsou definovány a vysvětleny klíčové pojmy používané v souvislosti s elektronickým podpisem. V první části kapitoly jsou uvedeny pojmy z § 2 zákona číslo 227/2000 Sb. o elektronickém podpisu (dále zákona o EP), vydaném ve Sbírce zákonů, částka 68, strana 3290 – 3297. V druhé části kapitoly je popsán postup získání certifikátu u certifikační autority, od žádosti, až po jeho obdržení. V následující kapitole jsou vysvětleny pojmy symetrické a asymetrické šifrování, hashovaní funkce. Poslední část kapitoly vysvětluje pojem infrastruktura veřejného klíče.

## 1.1 Elektronický podpis

Dle zákona o EP § 2 písm. a) se rozumí: „elektronickým podpisem údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě“ [47, s. 9503].

Za elektronický podpis je považován například podpis na klasické e-mailové zprávě, který je spíše informací a nevzbuzuje moc důvěry. Jestliže je třeba prokázat totožnost podepisující osoby při e-komunikaci, nelze jej použít.

## 1.2 Zaručený elektronický podpis

Dle zákona o EP § 2 písm. b) se rozumí: „zaručeným elektronickým podpisem elektronický podpis, který splňuje následující požadavky

1. je jednoznačně spojen s podepisující osobou,

2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,

3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,

4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat“ [47, s. 9503].

Zaručený EP je založen na metodě digitálního podpisu[1] a můžeme na něj nahlížet jako na číslo, které vytvoří podepisující osoba za pomocí prostředků pro vytváření elektronického podpisu

[1] Podpis vytvořený na základě asymetrické kryptografie.

a za pomoci zprávy, kterou tato osoba podepisuje. Číslo, které je takto vytvořeno je velmi veliké (např. 1024 bity) a jeho ověření je možné pouze za pomoci počítače [33].

Postup vytvoření zaručeného EP se skládá ze dvou částí:

- spočítá se otisk dokumentu za pomoci hashovací funkce (kapitola 1.3.2 asymetrické šifrování),

- dokument se zašifruje soukromým klíčem, který u sebe má osoba, která podpis vytváří. Zpráva je odeslána příjemci.

Postup příjemce zprávy opatřené EP:

- spočte otisk z přijaté zprávy,

- přijatý podpis ověří veřejným klíčem odesílatele.

Jestliže jsou výsledky obou předchozích bodů stejné, je identita podepsané osoby ověřena a navíc je doloženo, že nedošlo ke změně obsahu zprávy, je tedy zajištěna její integrita [2].

## 1.3 Elektronická značka

Dle zákona o EP § 2 písm. c) se rozumí: „elektronickou značkou údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují následující požadavky

1. jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu,

2. byly vytvořeny a připojeny k datové zprávě pomocí prostředku pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou,

3. jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat“ [47, s. 9503].

Můžeme říci, že elektronická značka je EP vytvořený pomocí prostředku pro vytváření elektronických značek, ale odlišuje se od EP po právní stránce. Zatímco EP vytváří jen fyzická osoba, elektronickou značku může využívat i právnická osoba nebo organizační složka státu. Využití elektronické značky je při výstupech z informačních systémů, v elektronických podatelnách úřadů, kdy je odesílateli potvrzováno, že jeho e-mail byl doručen na příslušnou adresu apod. [32].

## 1.4 Datová zpráva

Dle zákona o EP § 2 písm. d) se rozumí: „datovou zprávou elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou poštou“ [47, s. 9503].

Vše, co existuje v digitální podobě, lze považovat za datovou zprávu. Je to tedy posloupnost bitů – nul a jedniček a proto na ni můžeme nahlížet jako na číslo. Toto číslo je ale veliké a při podepisování elektronickým podpisem by tak docházelo k prodlevám, je tedy přepočteno na číslo kratší, které je vzhledem k podepisovanému dokumentu jedinečné a má pevnou délku. Tato matematicko-kryptografická metoda se nazývá hašování.

Před samotným odesláním datové zprávy je třeba pamatovat na to, že elektronické podatelny mají pro příjem datových zpráv stanoveny určitá pravidla, která se mohou i značně lišit, proto je vhodné předem zjistit, jak při odesílání postupovat. Mezi základní informace zveřejňované elektronickou podatelnou patří formát, velikosti datové zprávy nebo i možnosti jejího předání na datovém nosiči [32].

## 1.5 Podepisující osoba

Dle zákona o EP § 2 písm. e) se rozumí: „podepisující osobou fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby“ [47, s. 9503].

Podepisující fyzická osoba by se měla s obsahem datové zprávy před jejím podpisem seznámit, alespoň takto to předpokládá zákon o EP. Její povinnosti uvedeny v § 5. Jedná se zejména o možnost neoprávněného použití zaručeného EP, kdy je třeba neprodleně uvědomit poskytovatele certifikačních služeb.

Fyzická osoba, podepisující se jménem jiné fyzické či právnické osoby, musí být k tomuto zmocněna. Orgány veřejné moci mají na svých internetových stránkách u adres elektronických podatelen zveřejněny jména osob, které jsou oprávněny takto jednat [2].

## 1.6 Označující osoba

Dle zákona o EP § 2 písm. f) se rozumí: „označující osobou fyzická osoba, právnická osoba nebo organizační složka státu, která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou“ [47, s. 9503].

Na rozdíl od podepisující osoby, označující fyzická osoba označí datovou zprávu, aniž by zkontrolovala její obsah, § 3a odst. 2 zákona o EP [22].

## 1.7 Držitel certifikátu

Dle zákona o EP § 2 písm. g) se rozumí: „držitelem certifikátu fyzická osoba, právnická osoba nebo organizační složka státu, která požádala o vydání kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu pro sebe nebo pro podepisující nebo označující osobu a které byl certifikát vydán“ [47, s. 9503].

Držiteli certifikátu vyplývají ze zákona určité povinnosti a to podávání přesných, pravdivých a úplných informací poskytovateli certifikačních služeb.

Při žádosti o certifikát, je v bezpečnostních politikách jednotlivých certifikačních autorit požadováno prokázání totožnosti předložením dvou osobních dokladů. Za základní doklad je považován občanský průkaz. Zákon stanoví věkovou hranici pro držitele certifikátu a jeho způsobilost k provádění právních úkonů [10,24,26].

## 1.8 Certifikát

Dle zákona o EP § 2 písm. k) se rozumí: „certifikátem datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu, nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její identitu“ [47, s. 9504].

Certifikát je datový soubor, který obsahuje identifikační údaje držitele, jeho veřejný klíč, identifikaci vydavatele certifikátu, sériové číslo, pod kterým byl vydán (musí být jedinečné), dobu platnosti a další údaje vymezující způsob použití. Toto je stvrzeno digitálním podpisem certifikační autority.

Aby byl popis údajů na certifikátu snadno čitelný pro člověka je prováděn v jazyce ASN.1. Jestliže mají být údaje čitelné pro počítače, které mezi sebou komunikují, jsou tyto informace z jazyka ASN.1 převáděny do kódování BER. Informace se tak stávají pro člověka nečitelnými a nelze je zobrazit ani na displejích.

Rozšířeným typem certifikátu je atributový certifikát, kde jsou místo veřejného klíče uvedeny další rozšiřující identifikační údaje o držiteli. Tento certifikát je platný pouze s klasickým certifikátem, protože neprokazuje totožnost držitele [9].

## 1.9 Kvalifikovaný certifikát

Dle zákona o EP § 2 písm. k) se rozumí: „certifikát, který má náležitosti podle § 12 a byl vydán kvalifikovaným poskytovatelem certifikačních služeb [47, s. 9504].

Podle § 11 zákona o EP jej lze požívat v oblasti orgánů veřejné moci a mezi požadavky, které musí splňovat patří:

- certifikát je vydán jako kvalifikovaný,
- uvedení identifikace certifikační autority,
- uvedení identifikace osoby, které byl vydán,
- doba platnosti certifikátu,
- omezení transakcí pro použití certifikátu, pokud existují apod. [47].

## 1.10 Kvalifikovaný systémový certifikát

Dle zákona o EP § 2 písm. l) se rozumí: „certifikát, který má náležitosti podle § 12a a byl vydán kvalifikovaným poskytovatelem certifikačních služeb [47, s. 9504].

Mezi požadavky podle § 12a patří:

- označení, že byl vydán jako kvalifikovaný systémový certifikát,
- jednoznačná identifikace podepisující osoby,
- číslo kvalifikovaného systémového certifikátu,
- počátek a konec platnosti kvalifikovaného systémového certifikátu,
- omezení, pokud existují [47].

## 1.11 Kvalifikované časové razítko

Dle zákona o EP § 2 písm. r) se rozumí: „datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem [47, s. 9504].

Kvalifikované časové razítko obsahuje datum a čas vydání, číslo razítka, identifikaci třetí strany, která časové razítko vydala a otisk dat, ke kterým je vydáno. Další náležitosti jsou uvedeny v §12b zákona o EP.

Principielně lze popsat systém následně. Fyzická osoba, která vyžaduje ověření dokumentu, odešle tento k autorizaci certifikační autoritě prostřednictvím internetu, tato jej potvrdí a zašle zpět.

Dokument opatřený časovým razítkem nedokazuje to, že ho měla v držení určitá osoba (neobsahuje tedy identifikaci žadatele o časové razítko), ale to že v určitém čase existoval. K prokázání existence a držení dokumentu slouží tzv. DV-certifikát, nebo-li DV-časové razítko, které obsahuje položku „identifikace žadatele“.

Časová razítka se dají využívat při podpisu smluv v elektronické podobě, on-line obchodování nebo archivaci elektronickým dokumentů [9].

## 1.12 Elektronická podatelna

Dle zákona o EP § 2 písm. y) se rozumí: „pracoviště orgánu veřejné moci určení pro příjem a odesílání datových zpráv [47, s. 9504].

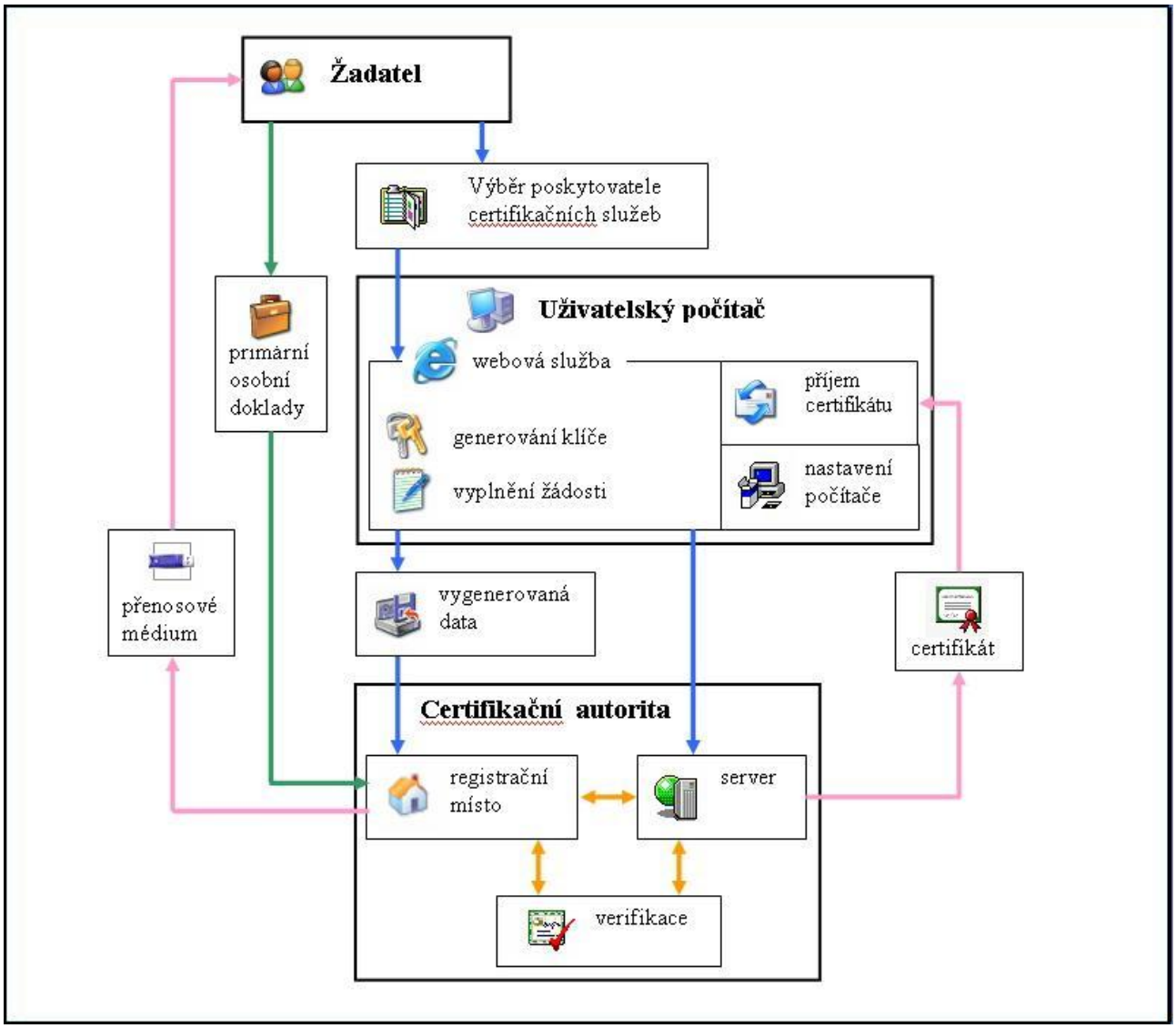
Provoz elektronických podatelen probíhá podle předem daných pravidel a instrukcí, která jsou nejčastěji shrnuta do „spisového řádu“. Pracovníkům podatelny z něho plynou povinnosti pro zacházení s elektronickými dokumenty při jejich odesílání, přijímání, ukládání a evidenci. Pro vybrané pracovníky i povinnost ověřit platnost elektronického podpisu a kvalifikovaného certifikátu, pokud jsou připojeny k datové správě.

Zákon upravuje některé další pojmy, jako například poskytovatel certifikačních služeb, kvalifikovaný poskytovatel certifikačních služeb a akreditovaných poskytovatel certifikačních služeb. Tyto pojmy jsou vysvětleny v následující kapitole číslo 3, která je celá věnována této problematice.

## 1.13 Získání kvalifikovaného certifikátu

Na počátku je třeba si určit k jakým účelům budeme elektronický podpis využívat. Před komunikací s druhou stranou je nutné nejprve ověřit, který certifikát považuje za důvěryhodný a poté zvolit poskytovatele. Pokud se rozhodneme pro komunikaci s orgány veřejné moci budeme potřebovat kvalifikovaný certifikát vydaný akreditovaným poskytovatelem certifikačních služeb.

Schéma na Obrázek 1 znázorňuje postup získání kvalifikovaného certifikátu od výběru poskytovatele, vyplnění a odeslání žádosti a vygenerování klíčů, přes návštěvu registračního místa, předložení žádosti, osobních dokladů a získání certifikátu, až po nainstalování certifikátu do počítače.




**Obrázek 1 Žádost o certifikát, zdroj autor**

### 1.13.1 Vygenerování žádosti a klíčů

Po výběru poskytovatele jsou dvě možnosti postupu. První je vyplnit žádost a vygenerovat klíče na webových stránkách poskytovatele. Druhá možnost je stáhnout aplikaci uveřejněnou na stránkách certifikační autority do počítače a vyplnit žádost a generovat klíče pomocí aplikace. Další postup je v obou případech společný. Dvojici klíčů je třeba nahrát na přenosové médium a provést zálohu, aby nedošlo k jejich ztrátě. První popsaná varianta je podstatně rychlejší pro ty klienty, kteří mají trvalý přístup k internetu. Pokud mají přístup k internetu omezen, je výhodnější použít druhou variantu, tedy pracovat za pomocí aplikace [10,24,26].

### 1.13.2 Registrační místo certifikační autority

Je to místo (pobočka) certifikační autority, na kterém poskytuje své služby. Dochází zde k osobnímu styku mezi klientem a poskytovatelem. Zde je třeba předložit žádost (v elektronické podobě) a doklady dle požadavku. Doklady, které je nutné předložit jsou uvedeny v certifikačních politikách jednotlivých poskytovatelů, podle typu zvoleného certifikátu. Je-li vše v pořádku je vydán certifikát z elektronické žádosti, dojde ke kontrole údajů a pokud vše souhlasí i k podpisu a převzetí certifikátu. Ten může být vydán na přenosovém médiu, čipové kartě nebo USB Tokenu [10,24,26].

### 1.13.3 Instalace certifikátu

Certifikát je nainstalován do počítače, na kterém byla vyplněna žádost a vygenerovány klíče, do úložiště pro soukromé klíče. Postup instalace je zvolen podle toho, jak bylo postupováno při vyplňování žádosti a generování klíčů. První možnost je přes webové stránky poskytovatele, druhá za pomocí aplikace [10,24,26].

## 1.14 Šifrování

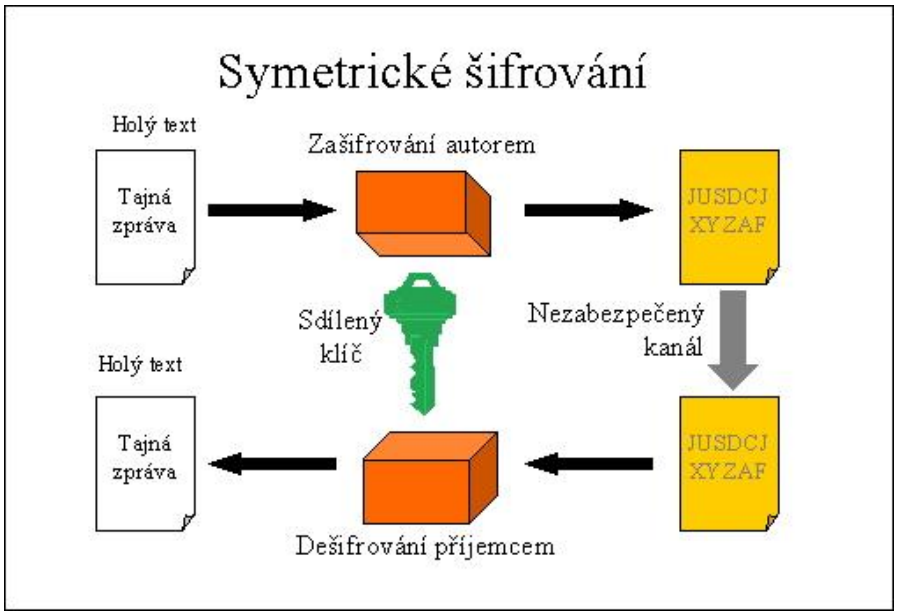
Systém EP je založen na šifrování. Samotné šifrování si můžeme představit jako proces, převedení čitelných dat na data nečitelná, tedy přístupná jen osobám, které znají heslo a nebo vlastní příslušný dešifrovací klíč. Ze zašifrovaných dat nelze vyčíst nic o charakteru a obsahu zprávy, která byla zašifrována. K šifrování, kromě vlastních dat, potřebujeme šifrovací algoritmus, což je matematický postup, podle kterého se šifrování provádí a šifrovací klíč, tedy unikátní sekvenci dat, která do šifrování vstupuje společně s vlastními daty. Nyní již lze provést zašifrování dat, tedy matematickou operaci, do které vstoupí vlastní data, plus šifrovací algoritmus, plus šifrovací klíč. Opačnou operací, tedy dešifrováním, vrátíme data do své původní podoby. V současnosti jsou využívány dva základní druhy šifrování – symetrické a asymetrické, případně je využívána kombinace těchto dvou typů [29].

### 1.14.1 Symetrické šifrování

Symetrické šifrování spočívá v tom, že zpráva je zašifrována i dešifrována stejným klíčem, který zná pouze určený okruh uživatelů. Nevýhodou je zde bezpečné předání klíče a jeho udržení v tajnosti při větším počtu uživatelů. Při vyzrazení klíče, byť jen jedním z nich, dojde k vyzrazení informací všech. Další velkou nevýhodou je počet všech klíčů, které by byly třeba při větším

rozšíření využívání. Tento počet lze vyjádřit vztahem n*(n-1)/2 klíčů pro n uživatelů. Následující Obrázek 2 ukazuje postup při zašifrování, odeslání a dešifrování zprávy.

Výhodou symetrického šifrování je jeho rychlost, protože je výpočetně méně náročné, na rozdíl od asymetrického šifrování.




**Obrázek 2 Symetrické šifrování, zdroj [31]**

Dnes jsou běžně požívány algoritmy s délkou klíče 128 bitů, které jsou:

- DES (Data Encryption Standard),
- IDEA (International Data Encryption Algorithm),
- RC2 a RC4 (Rivest Cipher) [31].

### 1.14.2 Asymetrické šifrování

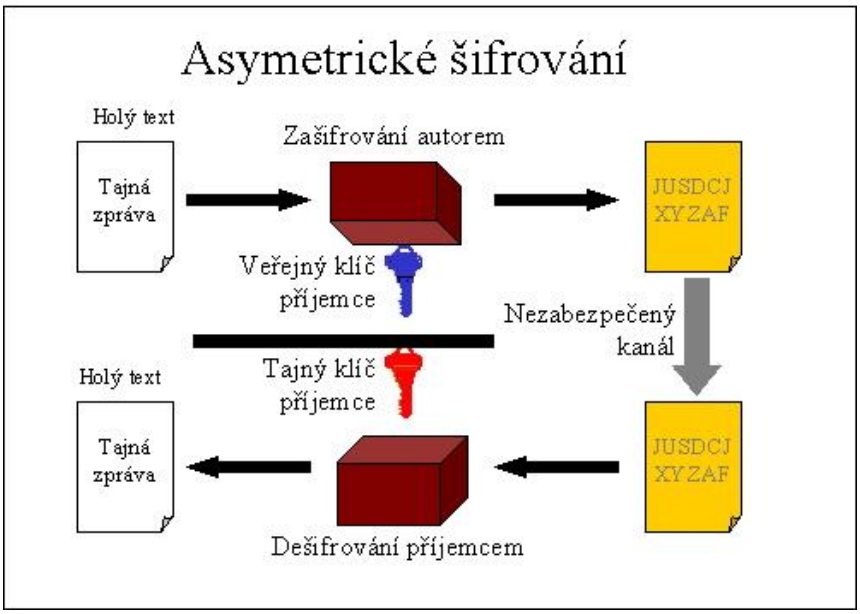
Při asymetrickém šifrování je využíván pár klíčů. Jeden pro šifrování (soukromý) a druhý pro dešifrování (veřejný). Zpráva je zašifrována soukromým klíčem, výsledek je připojen k textu jako podpis a vše odesláno. Na druhé straně osoba, která zprávu přijme, zjistí z textu jméno odesílající osoby a přes certifikační autoritu i její veřejný klíč. Za jeho pomoci dešifruje text zašifrovaný pomocí soukromého klíče a porovná ho s otevřeným textem. Jestliže se obojí shoduje, je zpráva doručena v pořádku. Ukázka průběhu asymetrického šifrování je na Obrázek 3.

Výhodou asymetrického šifrování je menší počet klíčů, který lze vyjádřit vztahem 2n při n uživatelích a odpadá i problém s bezpečným předáním klíče.

Nevýhodou je výpočetní náročnost a tím tedy i délka doby, po kterou je šifrování prováděno.

V současné době se používají tyto algoritmy:

- RSA (Rivest Shamir Adleman),
- DSS (Digital Signature Standard),
- EC (Eliptic Curve).




**Obrázek 3 Asymetrické šifrování, zdroj [31]**

U elektronického podpisu je postup obdobný, avšak není šifrován celý text, ale vytváří se otisk zprávy tzv. hash. Z libovolně dlouhé zprávy pak dostaneme řetězec, který má pevnou délku – 128 nebo 160 bitů. Při nepatrné změně zprávy pak dostaneme řetězec úplně jiný. Mezi používané hashovací algoritmy patří:

- MD5 (Message Digest 5) - výstup 128 bitů,
- SHA-1 (Secure Hash Algorithm) - výstup 160 bitů.

Při samotném podepisování je tedy postup následný. Ze zprávy je vypočítán hash, který je zašifrován soukromým klíčem, výsledek je připojen ke zprávě a odeslán. Příjemce pak vypočítá hash zprávy a za pomoci veřejného klíče odesílatele dešifruje přílohu a obojí porovná. Jsou-li oba dokumenty shodné, je vše v pořádku.

Požadavky kladené na hashovaní funkci [31]:

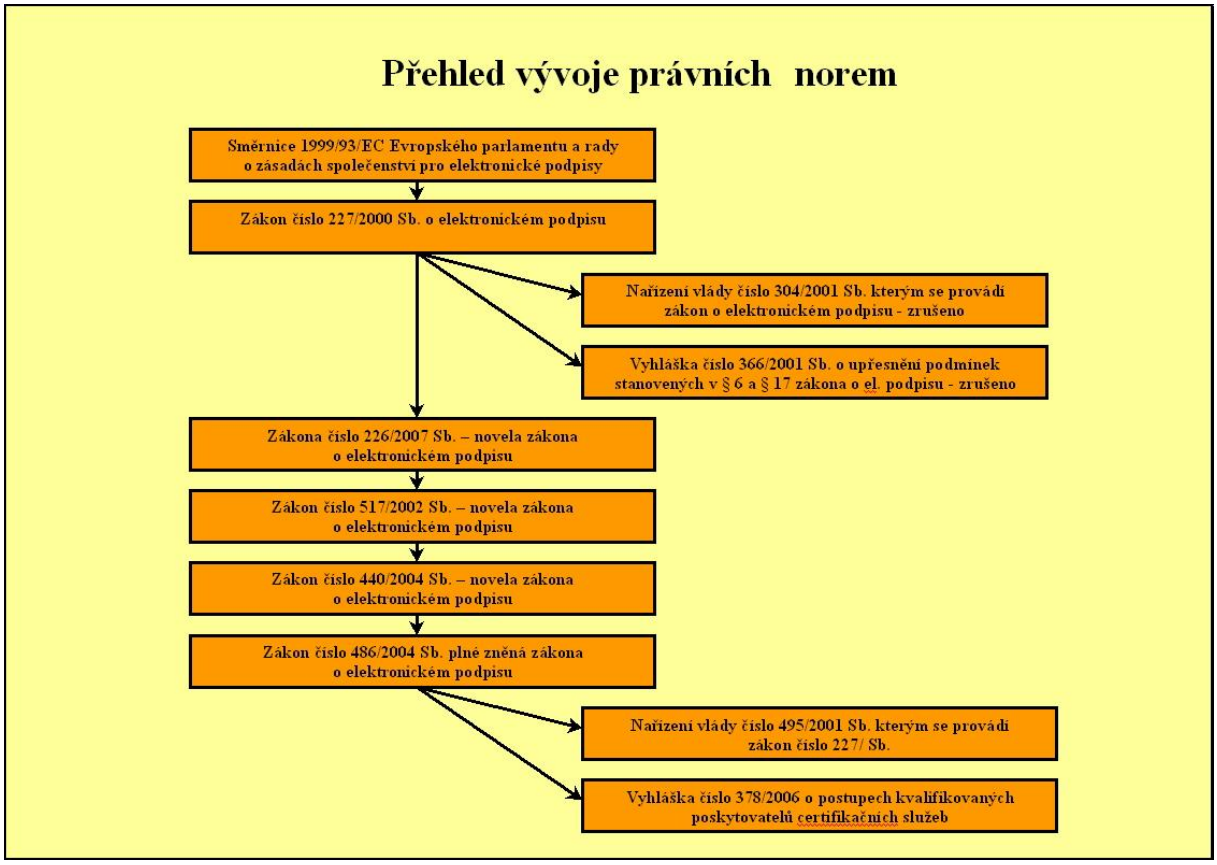
- výstup musí mít jednoznačně danou pevnou délku,
- u rozdílných vstupů nesmí být stejný výstup,
- známe-li výstup, nesmí být možné zpět dopočítat vstup.

## 1.15 Infrastruktura s veřejným klíčem

Infrastruktura s veřejným klíčem označována jako PKI (Public-Key Infrastructure) je pojem, se kterým se dnes běžně setkáváme v literatuře nebo na internetu. Doposud nebyl nikde přesně definován, ale můžeme si pod ním představit infrastrukturu veřejných klíčů, která se řídí určitými pravidly. Zahrnuje software, technologie a služby, které umožňují ochranu informačních systémů, elektronických transakcí a komunikace [38].

# 2. Právní úprava

Tato kapitola je věnována zákonům, které se týkají elektronického podpisu včetně novel, vyhlášek a nařízení podle kterých je zákon o elektronickém podpisu prováděn a dále zákony a předpisy s tímto zákonem bezprostředně související. Některé v současné době již neplatí, ale jsou zde uvedeny, aby bylo možné vidět postupný vývoj. Celý systém právních norem včetně novel a vyhlášek znázorňuje schéma na Obrázek 4.




**Obrázek 4 Přehled vývoje právních norem, zdroj autor**

## 2.1 Zákon číslo 227/2000 Sb. o elektronickém podpisu

Používání elektronického podpisu v České republice bylo upraveno zákonem číslo 227/2000 ze dne 29.června 2000 zákon o elektronickém podpisu. Při jeho tvorbě se vycházelo ze Směrnice 1999/93/EC Evropského parlamentu a Rady ze dne 13.prosince 1999 o zásadách Společenství pro elektronické podpisy, ve které bylo uloženo „členským státům Evropské unie přijmout právní a správní předpoklady nezbytné pro dosažení souladu s touto směrnicí (požadavky na právní akceptovatelnost e-podpisu, vytvoření dobrovolných akreditačních schémat, vzájemné uznávání certifikátů apod.)“ [2, s.60].

Elektronický podpis je tedy v legislativě postaven na roveň rukou psanému podpisu, vyjma těch případů, kdy je vyžadován rukou psaný dokument. Zákon vymezuje základní pojmy, stanovuje povinnosti osob využívajících elektronický podpis a podmínky pro poskytovatele certifikačních služeb. Zároveň dochází ke změně některých dalších zákonů[2], kde je dána možnost využívat elektronický podpis při právních úkonech, podáních, oznámeních, žádostech atd. [43].

## 2.2 Nařízení vlády číslo 304/2001 Sb., kterým se provádí zákon o elektronickém podpisu

V tomto nařízení vlády je orgánům veřejné moci, které přijímají ze zákona podání učiněná v elektronické podobě, dána povinnost zřídit elektronické podatelny a zajistit jejich činnost.

Elektronická podatelna, jako pracoviště orgánu veřejné moci, musí být vybavena potřebným zařízením připojeným k datové síti a programovým vybavením umožňujícím používání zaručeného EP, který je založený na kvalifikovaném certifikátu, vydaným akreditovaným poskytovatelem certifikačních služeb. Dále orgán veřejné moci musí pověřit zaměstnance vytvářením a ověřováním zaručeného EP a vybavit je k tomu potřebnými prostředky a kvalifikovaným certifikátem vydaným kvalifikovaným poskytovatelem certifikačních služeb. Elektronické adresy podatelen a seznamy kvalifikovaných certifikátů příslušných zaměstnanců musí být zveřejněny na úřední desce a nebo jiným způsobem umožňujícím dálkový přístup [19].

## 2.3 Vyhláška číslo 366/2001 Sb. o upřesnění podmínek stanovených v § 6 a § 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu

Vychází se zde z § 20 zákona o elektronickém podpisu, kde se Úřad pro ochranu osobních údajů zplnomocňuje vydávat vyhlášky k upřesňování podmínek stanovených v § 6 a § 17 zákona o elektronickém podpisu a je určen způsob, jak doložit jejich splnění. V § 6 zákona o EP jsou uvedeny povinnosti poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty a v § 17 zákona o EP jsou stanoveny požadavky na prostředky pro bezpečné vytváření a ověřování zaručených EP. Dále jsou uvedeny požadavky na nástroje elektronického podpisu a při vyhodnocování jejich shody, povinnost zveřejnit seznam těchto nástrojů ve Věstníku Úřadu pro ochranu osobních údajů [42].

[2] Dalšími zákony jsou zde rozuměny občanský zákoník, zákon o správě daní a poplatků, správní řád, občanský soudní řád, trestní řád, zákon o ochraně osobních údajů a zákon o správních poplatcích.

## 2.4 Zákon číslo 226/2002 Sb. a zákon číslo 517/2002 Sb. – novely zákona o EP

Zákon o elektronickém podpisu prošel několika významnými novelami. První novela zákon číslo 226/2002 ze dne 9.května 2002, kde dochází k doplnění § 11 o jednoznačné identifikovatelnosti osoby používající kvalifikovaný certifikát v oblasti orgánů veřejné moci. Druhá novela zákon číslo 517/2002 ze dne 14.listopadu 2002, kterým bylo zřízeno Ministerstvo informatiky a funkce Úřadu pro ochranu osobních údajů je zde nahrazena funkcí tohoto ministerstva [44,45].

## 2.5 Zákon číslo 440/2004 Sb. novela zákona o EP

Třetí nejvýznamnější novela zákon číslo 440/2004 ze dne 24. června 2004 původní zákon do značné míry rozšířila. Nově zavádí pojmy, jako jsou elektronická značka, označující fyzická osoba, držitel certifikátu, kvalifikovaný poskytovatel certifikačních služeb, kvalifikovaný systémový certifikát, data pro vytváření a ověřování elektronických značek, kvalifikované časové razítko, prostředek pro vytváření elektronických značek a elektronická podatelna. Jsou uvedeny povinnosti označující osoby a držitele certifikátu, dále povinnosti kvalifikovaného poskytovatele při vydávání kvalifikovaných certifikátů, vydávání kvalifikovaných razítek, podmínky pro rozšíření služeb, povinnosti při ukončení činnosti. Jaké náležitosti má mít kvalifikovaný systémový certifikát a časové razítko. Uznávání kvalifikovaných zahraničních certifikátů. Vymezuje právní delikty i přestupky související s činností kvalifikovaného poskytovatele certifikačních služeb [46].

## 2.6 Zákon číslo 486/2004 Sb. plné znění zákona o elektronickém podpisu

Všechny výše jmenované novely a původní zákon byly shrnuty do nového zákona číslo 486/2004 Sbírky, plné znění zákona o elektronickém podpisu.

## 2.7 Nařízení vlády číslo 495/2004 Sb., kterým se provádí zákon číslo 227/2000 Sb.

Toto nařízení vlády zrušuje nařízení číslo 304/2001 Sb., kterým se provádí zákon o EP. Určuje orgánům veřejné moci, které mají za povinnost přijímat a odesílat datové zprávy opatřené elektronickým podpisem, jak a za jakých podmínek provozovat elektronickou podatelnu a zveřejnit její adresu. Dále je dána lhůta, do které musí být adresa nahlášena Ministerstvu informatiky ČR (toto dnes již neexistuje a jeho funkci převzalo Ministerstvo vnitra ČR) [20].

## 2.8 Vyhláška číslo 496/2004 Sb. o elektronický podatelnách

Touto vyhláškou jsou určeny postupy při přijímání a odesílání datových zpráv na podatelnách orgánů veřejné moci. Dále povinnosti zaměstnanců při jejich evidenci a opatřování identifikátorem (podacím razítkem) a zaslání datové zprávy odesilateli o jejím doručení. U doručených zpráv opatřených zaručeným EP ověřit platnost kvalifikovaného certifikátu, případně uvědomit odesilatele, pokud bude certifikát v době doručení datové zprávy neplatný. Přílohou vyhlášky je postup při ověřování platnosti zaručeného elektronického podpisu a elektronické značky [40].

## 2.9 Zákon číslo 525/2004 Sb. úplné znění zákona číslo 101/2000 Sb. o ochraně osobních údajů

Ochrana osobních údajů je upřesněna v zákoně o EP v § 8, kde je stanoveno: „Ochrana osobních údajů se řídí zvláštním právním předpisem.“ [47, s. 9507]. Tím je míněn právě zákon o ochraně osobních údajů. Certifikační autority při poskytování svých služeb a svém působení zpracovávají osobní údaje svých klientů a proto se při jejich zpracování musí řídit tímto zákonem, aby nedošlo k jejich zneužití neoprávněnými osobami [48].

## 2.10 Vyhláška číslo 378/2006 Sb. o postupech kvalifikovaných poskytovatelů certifikačních služeb

Touto vyhláškou je zrušena vyhláška číslo 366/2001 Sb. o upřesnění podmínek stanovených v § 6 a § 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu. Vychází se zde z § 20 zákona o elektronickém podpisu, kde se Úřad pro ochranu osobních údajů zplnomocňuje vydávat vyhlášky k upřesňování podmínek stanovených v § 6 a § 17 zákona o elektronickém podpisu a je určen způsob, jak doložit jejich splnění. V § 6 zákona o EP uvedeny povinnosti poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty a v § 17 zákona o EP jsou stanoveny požadavky na prostředky pro bezpečné vytváření a ověřování zaručených EP. Dále jsou uvedeny požadavky na nástroje elektronického podpisu a při vyhodnocování jejich shody, povinnost zveřejnit seznam těchto nástrojů ve Věstníku Úřadu pro ochranu osobních údajů [41].

# 3. Certifikační autority

Certifikační autorita, nebo-li též poskytovatel certifikačních služeb, je subjekt, který zejména vydává certifikáty, spravuje je, zveřejňuje jejich seznamy a dále seznamy těch, které byly zneplatněny.

Certifikační autorita je definována v zákoně o EP v § 2, kdy pro účely tohoto zákona se rozumí:

- „poskytovatelem certifikačních služeb fyzická osoba, právnická osoba nebo organizační složka státu, která vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy,

- kvalifikovaným poskytovatelem certifikačních služeb poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty nebo kvalifikované systémové certifikáty nebo kvalifikovaná časová razítka nebo prostředky pro bezpečné vytváření elektronických podpisů (dále jen "kvalifikované certifikační služby") a splnil ohlašovací povinnost podle § 6,

- akreditovaným poskytovatelem certifikačních služeb poskytovatel certifikačních služeb, jemuž byla udělena akreditace podle tohoto zákona“. [47, s. 9504].

V oblasti státní správy je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydané akreditovanými poskytovateli certifikačních služeb. Podmínky udělování akreditací k působení jako akreditovaný poskytovatel certifikačních služeb jsou uvedeny v zákoně o EP a uděluje je příslušné ministerstvo. V současné době se jedná o tři kvalifikované poskytovatele certifikačních služeb. Akreditace byly jednotlivým poskytovatelům postupně uděleny Úřadem pro ochranu osobních údajů a zveřejněny ve Věstníku tohoto úřadu číslo 16/2002, Ministerstvem informatiky České republiky[3] a zveřejněny ve Věstníku tohoto ministerstva částka 2/2006. Protože došlo ke zrušení tohoto ministerstva[4] problematika s tímto spojená byla převedena pod Ministerstvo vnitra ČR[5].

V České republice byla udělena akreditace těmto certifikačním autoritám:

- První certifikační autorita, a.s.,
- ACA eIdentity a.s.,
- Post Signum QCA (Česká pošta s.p.).

[3] Změna v zákoně číslo 517/2002 Sb. ze dne 14.listopadu 2002, kdy pravomoci Úřadu pro ochranu osobních údajů přecházejí pod Ministerstvo informatiky.
[4] Zákon č. 110/2007 Sb. ze dne 19.dubna 2007 o některých opatřeních v soustavě ústředních orgánů státní správy, souvisejících se zrušením Ministerstva informatiky a o změně některých zákonů.
[5] Pod správu Ministerstva vnitra přešly i internetové stránky bývalého Ministerstva informatiky.

## 3.1 Hlediska pro hodnocení

Pro porovnání a následné hodnocení certifikačních autorit byla zvolena tato kriteria:

- dostupnost cetrifikační autority,

- produkty poskytované certifikační autoritou, identifikátor MPSV[6],

- doba platnosti certifikátu,

- cena certifikátu (s DPH),

- žádost o certifikát,

- doklady potřebné pro získání certifikátu,

- zneplatnění certifikátu,

- bezpečné uložení klíče.

## 3.2 První certifikační autorita a.s.

První CA byla založena počátkem roku 2001 jako dceřiná společnost PVT a.s.. V současné době je vlastněna několika společnostmi: Česká spořitelna a.s., Československá obchodní banka a.s., Telefónica O2 Czech Republic a.s., Asseco a.s. a Státní tiskárna cenin s.p.. Své služby poskytuje v České i Slovenské republice a má zde více něž 300 registračních míst (dále jen RM). Jako jediná ze tří srovnávaných poskytuje službu kvalifikovaných časových razítek a testovací certifikát. Dále nabízí bezpečné uložení dat na čipové kartě [26]. Další porovnávací kritéria jsou uvedena v následující Tabulka 1.

**Tabulka 1 Hlediska hodnocení - První certifikační autorita a.s., zdroj vlastní – upraveno na základě [26]**

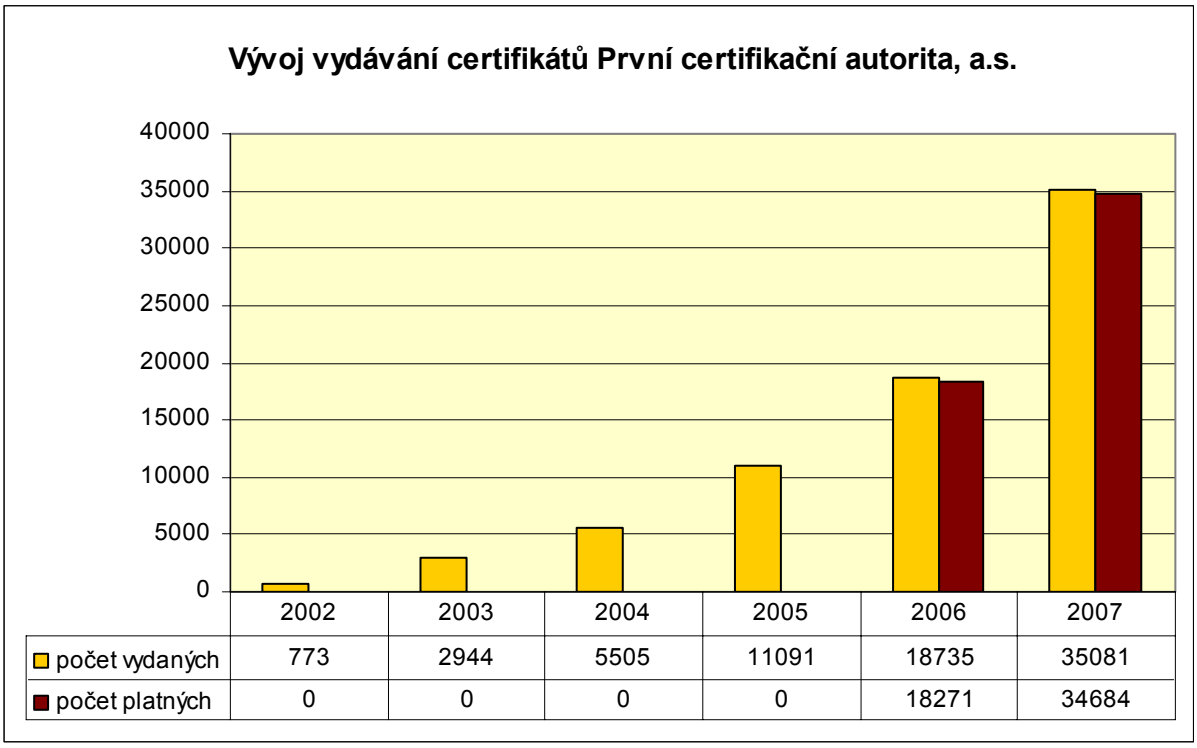
| První certifikační autorita a.s. | |
|---|---|
| **dostupnost certifikační autority** | |
| sídlo | Podvinný mlýn 2178/6, Praha 9 - Libeň |
| internetové stránky | http://www.ica.cz/ |
| informace | e-mail: info@ica.cz |
| registrační místa | více než 200 míst (na pobočkách Československé obchodní banky a.s., některá pracoviště krajských úřadů další) |
| mobilní RM | dle požadavků zákazníka |
| klientské RM | dle požadavků klienta na místě jím určeném |

[6] Identifikátor MPSV je jedinečná identifikace občana vůči Ministerstvu práce a sociálních věcí, České správě sociálního zabezpečení a Úřadu práce, je to obdoba rodného čísla, ale nelze z něho přečíst datum narození a pohlaví. Jedná se o deseticiferné číslo o rozsahu 1 100 100 100 až 2 294 967 295.

| | |
|---|---|
| **produkty poskytované certifikační autoritou, identifikátor MPSV** | |
| produkty | Testovací certifikáty |
| | Kvalifikované certifikáty |
| | Komerční certifikáty |
| | Kvalifikované systémové certifikáty |
| | Kvalifikovaná časová razítka |
| identifikátor MPSV | ano |
| **doba platnosti certifikátu** | |
| 14 dnů | testovací certifikát |
| 6 měsíců | komerční certifikáty s 512 bitovým kryptografickým klíčem |
| 12 měsíců | všechny ostatní certifikáty |
| **cena certifikátu (s DPH)** | |
| Kvalifikované certifikáty | |
| 752,00 Kč | typ Standard |
| 1 728,00 Kč | typ Komfort - prvotně |
| 752,00 Kč | typ Komfort - opakovaně |
| Kvalifikované systémové certifikáty | |
| 780,00 Kč | typ Standard |
| 1 756,00 Kč | typ Komfort - prvotně |
| 780,00 Kč | typ Komfort - opakovaně |
| 390,00 Kč | podpisový certifikát ke kvalifikovanému systémovému certifikátu |
| Komerční certifikáty | |
| 322,00 Kč | typ Standard (6 měsíců) |
| 580,00 Kč | typ Standard (12 měsíců) |
| 1 556,00 Kč | typ Komfort - prvotně |
| 580,00 Kč | typ Komfort - opakovaně |
| 1 073,00 Kč | certifikát pro server (6měsíců) |
| 1 931,00 Kč | certifikát pro server (12měsíců) |
| Kvalifikovaná časová razítka<br>informace o cenách na e-mailu tsa@ica.cz | |
| **získání certifikátu** | |
| testovací certifikát | prakticky okamžitě po odeslání žádosti na e-mailovou adresu |
| ostatní certifikáty | žádost on-line přes webové stránky nebo za pomoci aplikace NewCert<br>pokud není možnost on-line |
| **doklady potřebné pro získání certifikátu** | |
| testovací certifikát | nepožadovány |
| ostatní certifikáty | |
| fyzická osoba nepodnikající | občanský průkaz a další doklad k ověření totožnosti |
| fyzická osoba podnikající | občanský průkaz a další doklad k ověření totožnosti |
| právnická osoba a organizační složka státu | originál, nebo notářsky ověřenou kopii živnostenského listu, nebo jiný obdobný doklad o zřízení, doklad nebo plnou moc opravňující k jednání, občanský průkaz a další doklad k ověření totožnosti |
| **zneplatnění certifikátu** | |
| elektronicky, za pomoci hesla ke zneplatnění<br>osobně u registrační autority<br>doporučenou zásilkou do místa registrační autority | |
| **bezpečné uložení klíče** | |
| ano | čipová karta |

Na základě materiálů poskytnutých První certifikační autoritou a.s. byl vytvořen graf vývoje vydávání certifikátů touto autoritou. Počet vydaných certifikátů je od března roku 2002 do konce roku 2007. Celkem bylo za toto období vydáno 74 129 kvalifikovaných certifikátů. Počet platných

certifikátů ke konci měsíce autorita sleduje až od roku 2006 [36]. Z Graf 1 je vidět každoroční strmý nárust počtu vydaných certifikátů, z čehož vyplývá, že společnost upevňuje své postavení na trhu.




| | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 |
|---|---|---|---|---|---|---|
| počet vydaných | 773 | 2944 | 5505 | 11091 | 18735 | 35081 |
| počet platných | 0 | 0 | 0 | 0 | 18271 | 34684 |

**Graf 1 Vývoj vydávání certifikátů První certifikační autorita a.s., zdroj vlastní – upraveno na základě [36]**

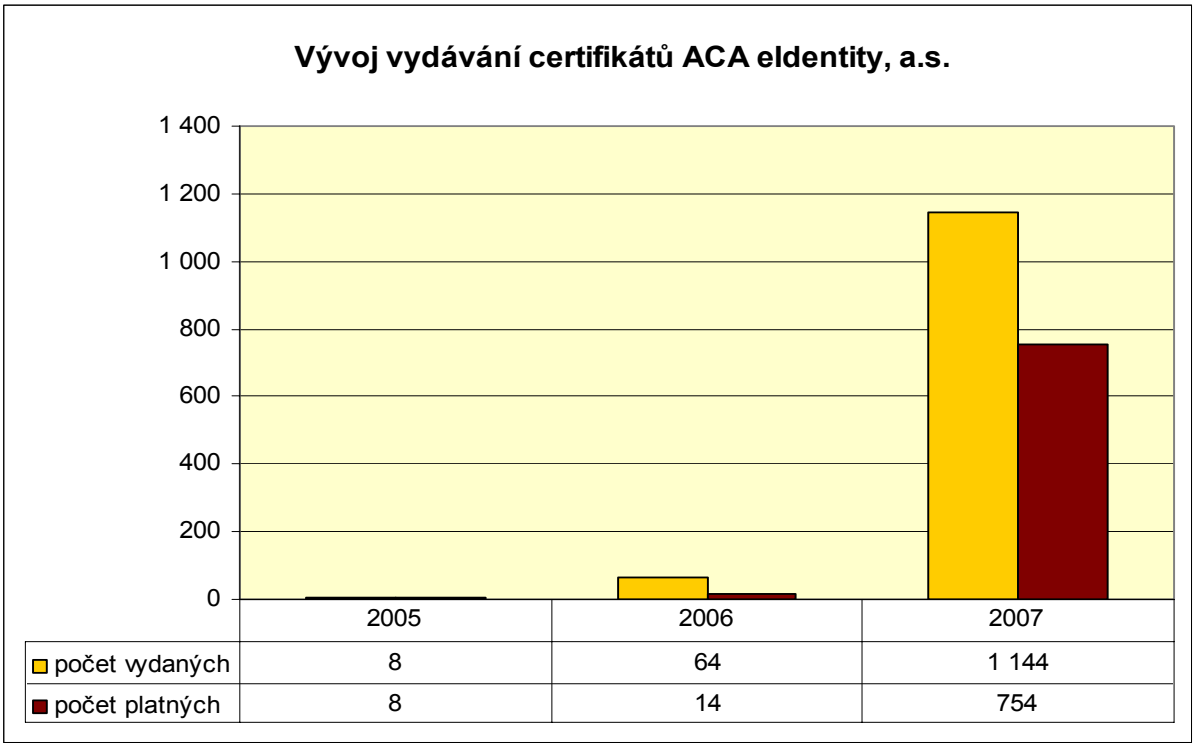
## 3.3 ACA eIdentity a.s.

Tato společnost vznikla v roce 2004 a zaměřila se na poskytování služeb v oblasti správy elektronické identity. Při srovnání poskytovaných služeb nebyly nalezeny větší rozdíly, jež by tuto společnost výrazně odlišovaly od dvou zbývajících. Nevýhodou se zde může jevit pouze jedno registrační místo [10]. Porovnávací kritéria jsou uvedeny v Tabulka 2.

Data o vydávání kvalifikovaných certifikátů touto certifikační autoritou byla poskytnuta Ministerstvem vnitra ČR, protože certifikační autorita data o vydávání certifikátů neposkytuje. Celkem bylo za období od roku 2005 do konce roku 2007 vydáno 1 216 kvalifikovaných certifikátů [14]. Vývoj vydávání certifikátů je znázorněn v Graf 2, z něhož je patrné založení společnosti před rokem 2005, v roce 2006 je počet vydaných certifikátů velmi nízký. Tento stav může být způsoben nedůvěrou klientů, případně jediným registračním místem. V roce 2007 je již viditelný nárůst klientely.

**Tabulka 2 Hlediska hodnocení - eIdentity a.s., zdroj vlastní – upraveno na základě [10]**

| ACA eIdentity a.s. | |
|---|---|
| **dostupnost certifikační autority** | |
| sídlo | Vinohradská 184, Praha 3 |
| internetové stránky | http://www.eidentity.cz, http://www.ie.cz |
| informace | e-mail: info@eidentity.cz, nebo info@ie.cz |
| registrační místa | 1 pevné na adrese společnosti |
| mobilní | dle požadavků zákazníka |
| **produkty poskytované certifikační autoritou, identifikátor MPSV** | |
| produkty | Kvalifikované certifikáty |
| | Kvalifikované certifikáty s vyznačením identifikátoru MPSV |
| | Kvalifikované certifikáty s vyznačením pracovní pozice v organizaci |
| | Kvalifikované systémové certifikáty |
| | Komerční certifikáty pro elektronický podpis |
| | Komerční certifikáty pro šifrování zpráv |
| | Komerční certifikáty pro identifikaci |
| | Komerční serverové certifikáty |
| identifikátor MPSV | ano |
| **doba platnosti certifikátu** | |
| 12 měsíců | všechny certifikáty |
| **cena certifikátu (s DPH)** | |
| Akreditované služby | |
| 702,00 Kč | Kvalifikovaný certifikát |
| 3 451,00 Kč | Kvalifikovaný systémový certifikát |
| Ceny komerčních služeb | |
| 238,00 Kč | Komerční certifikát (k již vydanému kvalifikovanému certifikátu) |
| 752,00 Kč | Komerční serverový certifikát (k již vydanému kvalifikovanému systémovému certifikátu) |
| Balíčky služeb | |
| 821,00 Kč | Balíček kvalifikovaného certifikátu a k němu vydaného komerčního certifikátu |
| 3 827,00 Kč | Balíček kvalifikovaného systémového certifikátu a k němu vydaného komerčního serverového certifikátu |
| **získání certifikátu** | |
| testovací certifikát | není v nabídce |
| certifikáty | žádost on-line přes webové stránky |
| **doklady potřebné pro získání certifikátu** | |
| fyzická osoba nepodnikající | občanský průkaz a další doklad k ověření totožnosti |
| fyzická osoba podnikající | občanský průkaz a další doklad k ověření totožnosti |
| právnická osoba a organizační složka státu | originál, nebo notářsky ověřenou kopii živnostenského listu, nebo jiný obdobný doklad o zřízení, doklad nebo plnou moc opravňující k jednání, občanský průkaz a další doklad k ověření totožnosti |
| **zneplatnění certifikátu** | |
| elektronicky po přihlášení ke svému účtu<br>písemnou žádostí, zaslanou nebo osobně předanou registrační autoritě | |
| **bezpečné uložení klíče** | |
| ano | není v nabídce |




**Graf 2 Vývoj vydávání certifikátů ACA e Ientity a.s., zdroj vlastní – upraveno na základě [14]**

## 3.4 PostSignum QCA

Tento poskytovatel je kvalifikovanou certifikační autoritou České pošty s.p.. Zaměřuje se na dvě odlišné skupiny zákazníků – organizace a nepodnikající fyzické osoby. Obdobně jsou rozdělena i registrační místa. Obchodní RM, sloužící pro uzavírání smluv s právnickými osobami a zavádění zákazníků a žadatelů do systému a kontaktní místo, kde jsou vydávány a zneplatňovány certifikáty a uzavírány smlouvy s fyzickými osobami. Výhodou je zde nízká pořizovací cena certifikátu a v současné době nově poskytovaná služba – čipová karta pro bezpečné uložení klíče [24]. Hlediska hodnocení jsou uvedena v následující Tabulka 3.

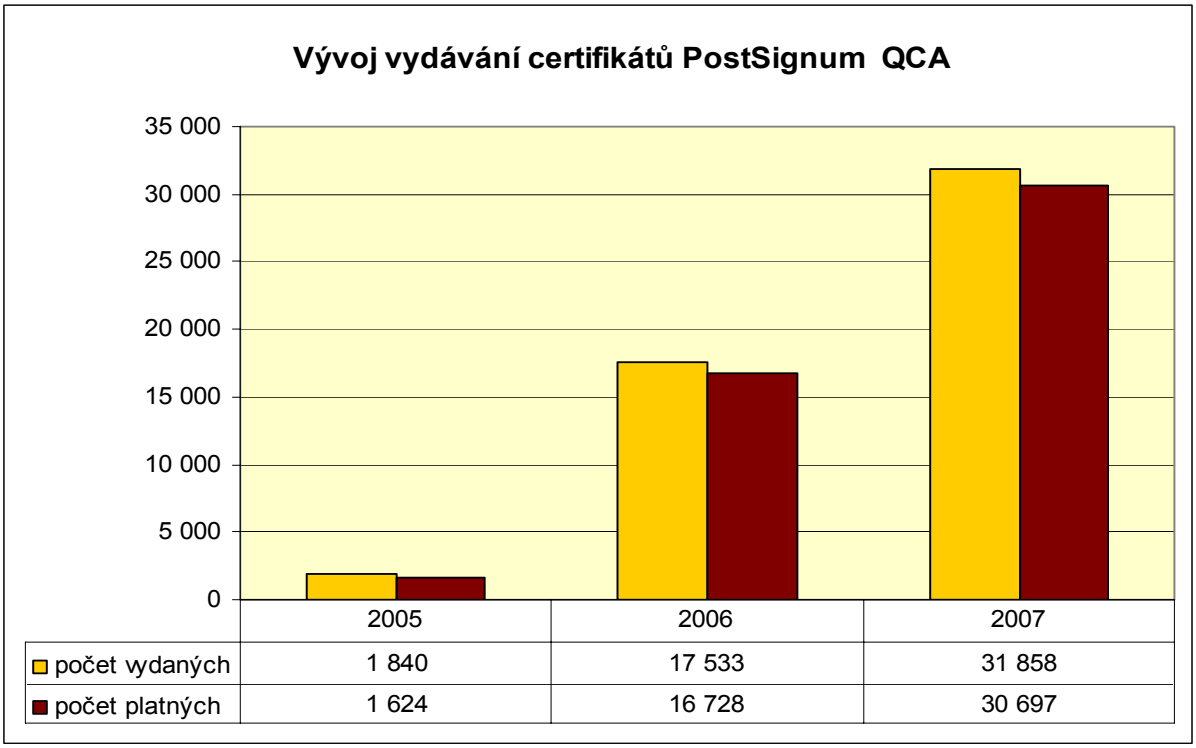
Vývoj vydávání certifikátů této autority je vidět v následujícím Graf 3. Jde o období 2005 až 2007, kdy bylo celkem vydáno 51 231 kvalifikovaných certifikátů. Z grafu je dále patrné, že certifikační autorita působí na trhu od roku 2005 a počty vydaných certifikátů každoročně stoupají. Mimo základních údajů týkajících se počtu vydaných a platných certifikátů byly poskytnuty další velmi podrobné údaje týkající se podílu jednotlivých typů certifikátů na celkovém vydaném množství. Počet platných kvalifikovaných certifikátů v roce 2007 podle jednotlivých typů je v Příloha 1. Z grafu je patrné, že největší zastoupení, 91,577 %, mají zaměstnanecké certifikáty. Pro lepší přehlednost jsou v Příloha 2 znázorněny počty certifikátů bez nejvíce vydávaných certifikátů zaměstnaneckých. Nejmenší zastoupení, prakticky nulové (0,004 %), má elektronická

značka fyzické osoby. Zbývající tři typy – elektronický podpis fyzické osoby, elektronická značka organizace a služební certifikáty jsou zastoupeny 8,419 % [37].

**Tabulka 3 Hlediska hodnocení - PostSignum QCA, zdroj vlastní – upraveno na základě [24]**

| **PostSignum QCA (elektronická služba České pošty)** | |
|---|---|
| **dostupnost certifikační autority** | |
| sídlo | Česká pošta s.p., Politických vězňů 909/4, Praha 1 |
| internetové stránky | http://qca.postsignum.cz/ |
| informace | e-mail: helpdesk-ca@cpost.cz |
| registrační místa | více jak 70 – spíše pro fyzické osoby |
| obchodní RM | 7 - spíše pro právnické osoby |
| mobilní | dle požadavků zákazníka |
| **produkty poskytované certifikační autoritou, identifikátor MPSV** | |
| produkty | Certifikáty pro ověření elektronického podpisu zaměstnance |
| | Certifikáty organizace pro ověření elektronické značky |
| | Certifikáty pro ověření elektronického podpisu fyzické osoby |
| | Certifikáty pro ověření elektronické značky fyzické osoby |
| identifikátor MPSV | ano |
| **doba platnosti certifikátu** | |
| 12 měsíců | všechny certifikáty |
| **cena certifikátu (s DPH)** | |
| 190,00 Kč | Certifikáty pro ověření elektronického podpisu zaměstnance |
| 2 856,00 Kč | Certifikáty organizace pro ověření elektronické značky |
| 190,00 Kč | Certifikáty pro ověření elektronického podpisu fyzické osoby |
| 2 856,00 Kč | Certifikáty pro ověření elektronické značky fyzické osoby |
| **získání certifikátu** | |
| testovací certifikát | není v nabídce |
| certifikáty | generování žádosti přes webové stránky |
| **doklady potřebné pro získání certifikátu** | |
| fyzická osoba nepodnikající | vyplněná objednávka, zákaznický formulář, elektronická žádost, dva osobní doklady |
| fyzická osoba podnikající | vyplněná objednávka, zákaznický formulář, živnostenský list (zřizovací doklad), elektronická žádost, jeden osobní doklad |
| právnická osoba a organizační složka státu | vyplněná objednávka ve dvou vyhotoveních, originál nebo potvrzená kopie z obchodního rejstříku, doklad nebo plnou moc opravňující k jednání, vytištěný a žadateli podepsaný seznam žadatelů, doklad totožnosti osoba, která byla určena k zastupování |
| **zneplatnění certifikátu** | |
| na kontaktním místě osobně<br>telefonicky<br>e-mailem | |
| **bezpečné uložení klíče** | |
| ano | čipová karta[7] |

[7] Čipové karty jsou nabízeny od 2. ledna 2008.




**Graf 3 Vývoj vydávání certifikátů PostSignum QCA, zdroj vlastní – upraveno na základě [37]**

## 3.5 Srovnání nabízených služeb

Srovnání nabízených služeb bylo provedeno podle kriterií uvedených v kapitole 3. Všechny tři certifikační autority provozují internetové stránky, kde byly nalezeny velmi podrobné informace o poskytovaných službách, jako jsou certifikační politiky, typy vydávaných certifikátů, evidence platných certikátů, evidence zneplatněných certifikátů, postupy při žádosti o certifikát, seznamy registračních míst apod.. Mimo to, jsou zde zřízeny e-mailové adresy pro podávání dalších informací, jako je technická podpora, např. pokud se nedaří instalace certifikátu. Nejvíce registračních míst bylo zjištěno u První certifikační autority a.s., více jak 200, jako druhá v pořadí je PostSignum QCA, s více jak 70 RM. Pouze jediné registrační místo má ACA eIdentity a.s.. Všechny tři společnosti provozují mobilní RM dle potřeb zákazníka a na přání zákazníka mohou zřídit klientské RM v místě, kde si zákazník určí.

Produkty poskytované registrační autoritou, identifikátory MPSV – poskytované produkty jsou prakticky na stejné úrovni. Na první pohled se od sebe liší v obchodním názvu, ale prakticky se jedná o kvalifikované certifikáty a kvalifikované systémové certifikáty. Výjimkou je Kvalifikované časové razítko První CA a.s. a testovací certifikát. Identifikátory MPSV, které jsou vyžadovány Ministerstvem práce a sociálních věcí, Českou správou sociálního zabezpečení a Úřadem práce, jsou poskytovány všemi třemi autoritami.

Doba platnosti certifikátu je u všech tří certifikačních autorit 12 měsíců, výjimkou je komerční certifikát První CA a.s. s 512 bitovým kryptografickým klíčem, který má dobu platnosti 6 měsíců a testovací certifikát s dobou platnosti 14 dnů.

Nejnižší cena kvalifikovaného certifikátu byla zaznamenána u certifikační autority PostSignum QCA a.s., která v roce 2007 činila 190,-- Kč, oproti cenám kvalifikovaných certifikátů zbývajících dvou certifikačních autorit. Ceny certifikátů těchto společností jsou téměř na stejné úrovni. U certifikační autority ACA eIdentity a.s. je to cena 702,-- Kč a u První certifikační autority a.s. 752,-- Kč za kvalifikovaný certifikát.

Žádost o certifikát se u První certifikační autority a.s. a ACA eIdentity a.s. vyplňuje na internetových stránkách příslušné autority a přes internet je odeslána certifikační autoritě. Tento postup je výhodný pro klienty s trvalým připojením k internetu. Pro klienty, kteří nemají trvalé připojení k internetu je např. společností První certifikační autorita a.s. nabízena aplikace NewCert, za jejíž pomoci je možné vyplnit žádost o certifikát. U certifikační autority PostSignum QCA a.s. je žádost na internetu také vytvářena, ale poté ji je třeba nahrát na přenosové médium a doručit na kontaktní místo této autority.

Doklady, potřebné pro získání certifikátu, jsou zveřejněny v certifikačních politikách certifikačních autorit podle jednotlivých typů certifikátů. Až na nepatrné rozdíly jsou u všech tří autorit totožné. Mezi základní požadované doklady patří občanský průkaz, plus další doklad k ověření totožnosti (např. cestovní pas). Právnické osoby nebo organizační složky státu musí mimo jiné doložit originál nebo notářsky ověřenou kopii živnostenského listu nebo jiný doklad o zřízení a plnou moc opravňující k jednání.

Bezpečné uložení klíče na čipové kartě je nabízeno dvěma poskytovateli a to První certifikační autoritou a.s. a od 2. ledna 2008 také PostSignum QCA a.s.

Pro srovnání jednotlivých certifikačních autorit, jako vydavatelů kvalifikovaných certifikátů, je v Příloha 3 uveden graf vývoje počtu platných kvalifikovaných certifikátů za období 2006 a 2007. Jedná se období, kdy všechny tři certifikační autority působí na trhu společně. Z tohoto grafu je patrné, že nejmenší počet zákazníků má ACA eIdentity a.s. a zbývající dvě certifikační autority QCA PostSignum a.s. a První certifikační autorita a.s. ovládají trh s kvalifikovanými certifikáty.

# 4. Současný stav využití elektrického podpisu

Zaručené EP založené na kvalifikovaných certifikátech vydané akreditovanými poskytovateli certifikačních služeb jsou využívány při elektronické komunikaci občanů nebo organizací se státní správou a uvnitř státní správy, kdy jednotlivé úřady elektronicky komunikují navzájem mezi sebou. Tato komunikace ve většině případů probíhá prostřednictvím e-podatelny, v některých případech jsou uvedeny elektronické adresy. Pro zmapování současného stavu byly využity internetové stránky jednotlivých orgánů státní správy. Tyto byly navštíveny a rozděleny do následujících kategorií. Pro další popis současného stavu byly internetové stránky orgánů státní správy, kde je možné podávat e-podání „hromadně".

Navštívené internetové stránky úřadů státní správy lze rozdělit do následujících kategorií:

1. Je uvedena adresa e-podatelny nebo adresa pro příjem datových zpráv, ale další podmínky nejsou blíže specifikovány.

2. Je uvedena adresa e-podately pro příjem datových zpráv, blíže specifikovány podmínky pro jejich přijímání, stanoveno, které druhy datových zpráv musí být podepsány zaručeným EP a vyjmenovány certifikační autority, které akceptují.

Druhy datových zpráv, které jsou nejčastěji přijímány:

- Datové zprávy bez EP
    - běžná e-mailová komunikace,
    - žádost o poskytnutí informací podle zákona č. 106/1999 Sb. o svobodném přístupu k informacím (někde vyžadování i EP).
- Datové zprávy opatřené zaručeným EP
    - podání podle zákona č. 500/2004 Sb. správní řád (§37),
    - stížnosti, oznámení a podněty podle zákona č. 500/2004 Sb. správní řád (§175),
    - datové zprávy, které jsou specifické pro určité státní orgány a jejich přijímání je výslovně uvedeno v informacích vztahujících se k e-podatelně a nebo k e-podáním[8].

3. Přijímají e-podání „hromadně" a to buď přímo na svých internetových stránkách v e-podatelně a nebo je zde zveřejněn odkaz na stránky, kde je možné takové podání učinit. K podpisu těchto

[8] Agentura ochrany přírody a krajiny ČR poskytuje datové zdroje AOPK ČR ve formě databází, vrtev GIS a jejich atributových informací, rastrových formátů apod. na základě e-žádosti, která je opatřená elektronickým podpisem.

podání je třeba EP založený na kvalifikovaném certifikátu vydaný akreditovaným poskytovatelem certifikačních služeb. Seznamy poskytovatelů, kteří jsou akceptováni, jsou uvedeny na těchto stránkách. Spadají sem i e-podání kategorie 2.

## 4.1 Server českého soudnictví justice.cz

Nachází se na adrese http://portal.justice.cz/ a je společný pro ministerstvo spravedlnosti, soudy, státní zastupitelství, rejstřík trestů, justiční akademii, institut pro kriminologii a sociální prevenci, probační mediační službu a vězeňskou službu. E-podání je možné učinit přes rozbalovací nabídku *Rejstřík trestů, Elektronická podatelna, Plné el. podání* a dále dle výběru a nebo přes rozbalovací nabídku *E-podatelna, Nové podání* a pokračovat pomocí průvodce [13].

### 4.1.1 Rejstřík trestů

Vyplňují se jednotlivé žádosti – formuláře a ty jsou podepsány a odeslány. Při vyplňování dochází průběžně ke kontrole vpisovaných údajů, např. tvar rodného čísla. U vyplňování adres je předdefinována nabídka měst, ulic, čísel popisných. Možnosti pro e-podání, které je možné učinit, jsou uvedeny v následující kapitole číslo 5. Pro komunikaci s Rejstříkem trestů lze využít následující možnosti [13]:

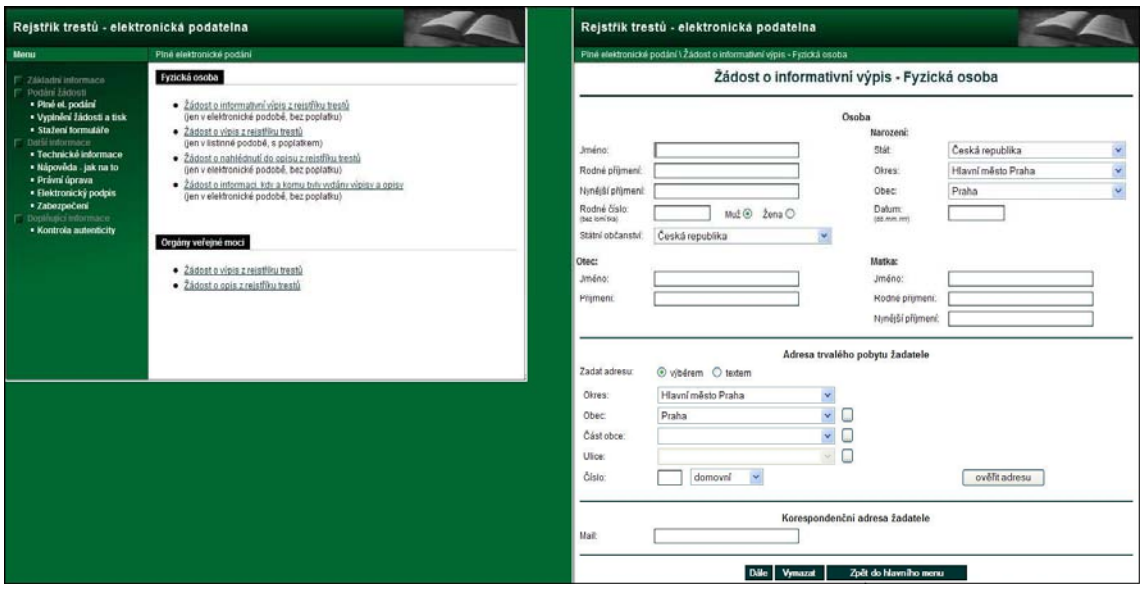
- komunikace přes webový formulář za pomoci internetového prohlížeče, formulář je před odesláním opatřen zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu, této možnosti se využívá např. je-li pro komunikaci s rejstříkem tretů pověřena jedna nebo dvě osoby určitého úřadu,
- komunikace prostřednictvím klienta webové služby, kdy převážně na serveru běží aplikace komunikující s Rejstříkem trestů, formulář je v tomto případě před odesláním opatřen elektronickou značkou založenou na kvalifikovaném systémovém certifikátu, tato možnost se využívá např. je-li pro komunikaci s rejstříkem trestů pověřeno více osob určitého úřadu.

Ukázka webového prostředí, ve kterém je vyplňován formulář je na následujícím Obrázek 5.

Od 1. července 2008 mohou orgány veřejné moci dle zákona číslo 124/2008 Sb. ze dne 19. března 2008, kterým se mění zákon číslo 269/1994 Sb. o Rejstříku trestů, vyžadovat výpis nebo opis z rejstříku trestů. Pro získání výpisu nebo opisu mohou využívat systém Czech POINT[9] nebo dálková přístup na serveru českého soudnictví justice.cz. Pro elektronickou komunikaci

[9] Czech POINT neboli Český podávací ověřovací informační národní terminál, je asistovaným místem výkonu veřejné správy, kde je možné získat a ověřit data z veřejných i neveřejných informačních systémů

je vyžadován kvalifikovaný EP pro pověřené zaměstnance a v kvalifikovaném zaměstnaneckém certifikátu musí být uvedeny další povinné údaje, jinak bude žádost Rejstříkem trestů zamítnuta.




**Obrázek 5 Ukázka webového prostřední pro e-podání, server českého soudnictví justice.cz, Rejstřík trestů, zdroj vlastní – upraveno na základě [27]**

Mezi další povinné údaje kvalifikovaného zaměstnaneckého certifikátu patří:

- označení orgánu veřejné moci,
- organizační útvar,
- zařazení zaměstnance.

Dále dochází ke změně pro správní orgány (přestupkové komise), které mohou také využívat dálkový přístup. Doposud mohly žádat o vydání výpisu nebo opisu pouze v listinné podobě. Náležitosti kvalifikovaného zaměstnaneckého certifikátu zůstávají stejné [13].

### 4.1.2 E-podatelna

Za pomoci interaktivních inteligentních formulářů je průběžně vyplňováno podání. Na každé stránce je možnost volby a podle zvolené možnosti je pokračováno na další nabídku. Nakonec je zobrazeno celé podání, poté podepsáno a odesláno. Ukázka prostředí aplikace, kde je možné učinit e-podání je na Obrázek 6.

Možnosti e-podání [13]:

- první podání k soudu – při návrhu na zahájení řízení a pokračovat dalším výběrem typu podání,
- další podání k soudu – soudní řízení probíhá a je známa spisová značka.


**Obrázek 6 Ukázka prostředí aplikace pro e-podání, server českého soudnictví justice.cz, e-podatelna, zdroj vlastní – upraveno na základě [13]**

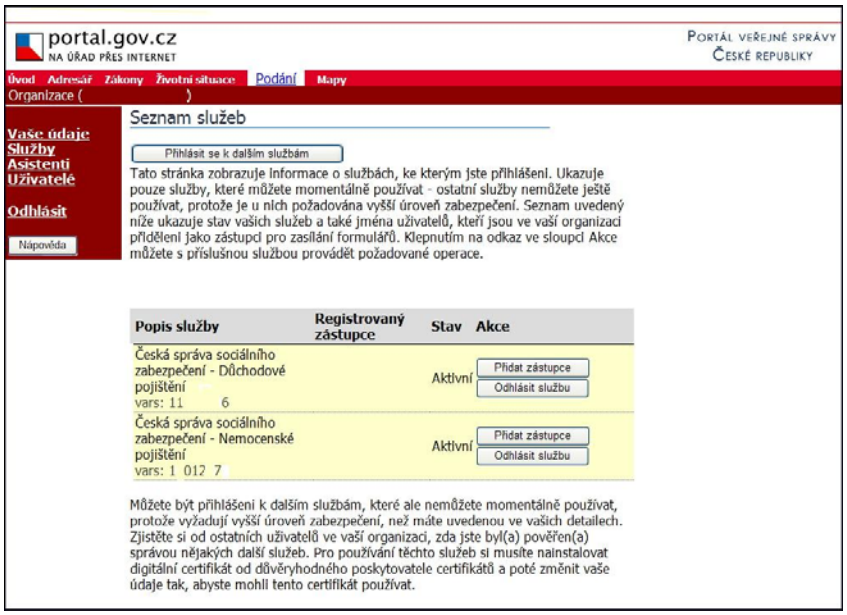
## 4.2 Daňový portál

Nachází se na adrese http://adisspr.mfcr.cz/ a slouží pro komunikaci s daňovou správou a k získávání informací z daňového řízení. E-podání lze učinit za pomoci interaktivních inteligentních formulářů přes rozbalovací nabídku *Elektronická podání pro daňovou správu* a pokračovat dle výběru. U většiny podání je vyžadován zaručený EP založený na kvalifikovaném certifikátu, kde tomu tak není, je uvedena lhůta, dokdy musí být chybějící údaje doplněny. Druhy e-podání, které je možné učinit a služby poskytované daňovým portálem, k jejichž používání je třeba vlastnit kvalifikovaný certifikát, jsou uvedeny v kapitole 5. Ukázka prostředí ve kterém jsou vyplňovány e-podání je na Obrázek 7 [8].


**Obrázek 7 Ukázka webového prostředí pro e-podání, daňový portál, zdroj vlastní – upraveno na základě [8]**

## 4.3 Portál veřejné správy České republiky

Nachází se na adrese http://portal.gov.cz/ a pro e-podání jej využívá více subjektů. Přes rozbalovací nabídku Podání, Dostupné elektronické služby je zde uvedena Česká správa sociálního zabezpečení, Ministerstvo průmyslu a obchodu, Ministerstvo financí10, Generální ředitelství cel, Ministerstvo dopravy a Ministerstvo životního prostředí. Jsou zde uvedeny souhrnné informace o typech podání a odkazy na internetové stránky jednotlivých úřadů. Prostředí webové služby je na Obrázek 8 [12].




**Obrázek 8 Ukázka webového prostředí pro přihlášení ke službám, portál veřejné správy, zdroj vlastní – upraveno na základě [12]**

### 4.3.1 Česká správa sociálního zabezpečení

Internetové stránky se nachází na adrese http://www.cssz.cz/ a v rozbalovací nabídce *e-podání* jsou uvedeny typy podání, které je možné podat elektronicky (více v následující kapitole 5). Pro e-podání je vyžadována osobní registrace klientů na místně příslušných Okresní (Pražské) správě, kde jim jsou přiděleny registrační údaje s jejichž pomocí se mohou přihlásit na Portálu veřejné správy. Dále je třeba sdělit identifikátory kvalifikovaného certifikátu – vystavitele a sériové číslo, protože v systému České správy sociálního zabezpečení slouží k identifikaci a autorizaci klienta. Jestliže je e-podání podepsáno platným kvalifikovaným certifikátem,jehož identifikátory klient nesdělil, dojde k jeho zamítnutí. Ukázka prostředí elektronického formuláře je na Obrázek 9 [35].

[10] Možnosti popsány výše v odstavci Daňový portál a následující kapitole číslo 5


**Obrázek 9 Ukázka prostředí elektronického formuláře, Česká správa sociálního zabezpečení, zdroj vlastní – upraveno na základě [35]**

### 4.3.2 Generální ředitelství cel, Celní správa České republiky

Na internetové adrese http://www.cs.mfcr.cz:80/ a přes rozbalovací nabídku *Clo, daně, obchod se zbožím, Spotřební daně, eDAP OnLine,* elektronické podání přiznání spotřební daně jsou uvedeny typy daňových přiznání, které lze podat elektronicky:

- DAP18, tj. daňové přiznání ke spotřební dani dle §18 zákona o SPD,
- DAP56, tj. daňové podání k přiznání nároku na vrácení spotřební daně dle §56 zákona o SPD (tzv. "teplo"),
- DAP57, tj. daňové podání k přiznání nároku na vrácení spotřební daně dle §57 zákona o SPD (tzv. "zelená nafta").

Pro e-podání je vyžadován:

- kvalifikovaný certifikát s bezvýznamovým identifikátorem MPSV,
- registrace na Portálu veřejné správy v aplikaci Elektronická podání,
- formuláře eDAP, které je možné stáhnout,
- program Adobe Reader 8.0 a vyšší, respektive Adobe Acrobat 8.0 a vyšší
- zásuvný modul (plug-in) pro propojení elektronických formulářů s Portálem veřejné správy a s následnou cestou zpracování formulářových údajů.

Před vyplněním formulářů eDAP je možné shlédnout animovaného průvodce, který uživatele seznámí se základními kroky při jejich vyplnění a pro úspěšné elektronické odeslání podepsaných dat. Ukázka elektronického formuláře je na Obrázek 10 [11].


**Obrázek 10 Ukázka prostředí elektronického formuláře, Celní správa ČR, zdroj vlastní – upraveno na základě [11]**

### 4.3.3 Ministerstvo životního prostředí

Pod ministerstvo životního prostředí Centrální ohlašovna znečištění na internetové adrese http://www.centralniohlasovna.cz/, která je informačním systémem shromažďujícím ohlašované údaje z oblasti životního prostředí. Uživatelé musí mít zřízen svůj účet a žádost o jeho zřízení se zasílá na e-mailovou adresu a musí být opatřena platným elektronickým podpisem. [5]

U zbývajících dvou ministerstev, tedy Ministerstva průmyslu a obchodu ČR a Ministerstva dopravy ČR nebyla zjištěna e-podání, kromě kategorie 2, u kterých by byl vyžadován elektronický podpis založený na kvalifikovaném certifikátu.

### 4.3.4 Český úřad zeměměřičský a katastrální

Dostupný na internetové adrese http://www.cuzk.cz/. Na stránkách je uveřejněn seznam e-podání, které musí být podepsány zaručeným elektronickým podpisem. Jedná se o:

- žádost o poskytnutí údajů z katastru nemovitostí,
- podání směřující k zápisu jiných údajů katastru nemovitostí podle § 6 katastrálního zákona,
- podání, rozhodnutí, potvrzení či jiná písemnost, na jejímž podkladě má být do katastru nemovitostí zapsána nebo z katastru nemovitostí vymazána poznámka.

Zároveň je zde i uvedeno, že formou elektronického podání nelze činit návrh na vklad a záznam věcných práv do katastru nemovitostí. [7]

# 5. Zhodnocení e-podání ve vybraných orgánech státní správy

Orgány státní správy (dále jen orgány) byly vybrány z třetí kategorie a to podle místa dostupnosti. Jedná se o následující:

- Okresní správa sociálního zabezpečení, pracoviště Pardubice (dále OSSZ PA),
- Celní správa České republiky, pracoviště Hradec Králové (dále CS HK),
- Celní správa České republiky, pracoviště Pardubice (dále CS PA).

Jednotlivé úřady byly navštíveny, ale potřebné podklady nebyly a nebo nemohly být poskytnuty. Přístup pracovníka OSSZ PA byl velmi vstřícný, ale bohužel část potřebných údajů není na OSSZ vedena. Potřebné údaje nebyly získány ani na CS HK, kde mi pracovníky bylo sděleno, že aplikace na e-podání není využívána a to z následujícího důvodu: k daňovému přiznání je třeba doložit přílohy a aplikace neumožňuje jejich vložení. Klient je tedy nucen přinést potřebné přílohy na pobočku a to již s sebou vezme i daňové přiznání. Údaje tedy nejsou k dispozici. CS PA údaje nesděluje.

Z výše uvedených důvodů byly prostřednictvím internetu osloveny jiné orgány státní správy a potřebné údaje byly poskytnuty od následujících orgánů:

- Ministerstvo financí České republiky (dále MF ČR),
- Česká správa sociálního zabezpečení (dále ČSSZ),
- Rejstřík trestů, Praha (dále RT).

Jelikož se jedná o naprosto odlišné oblasti, nelze prakticky nabízené možnosti pro elektronická podání mezi jednotlivými orgány srovnávat a v neposlední řadě samotné orgány shromažďují potřebné údaje podle oblasti svých zájmů. Vhodným společným kriteriem pro všechny tři oblasti, by bylo porovnání počtu ručních a elektronických podání. Ale bohužel, zatím co jsou počty elektronických podání vedeny velmi přesně, informace o počtech ručních podání prakticky neexistují. Ministerstvo financí ČR a Česká správa sociálního zabezpečení shromažďují převážně údaje týkající se počtu e-podání podle jednotlivých typů a let, kdežto Rejstřík trestů Praha se zaměřuje na údaje týkající se počtu e-podání podle jednotlivých žadatelů a let. Z výše uvedených důvodů byla zvolena tři kriteria společná pro všechny tři orgány státní správy, další kriteria byla volena podle individuelně podle jednotlivých posuzovaných oblastí.

Společná kriteria:

- počet e-podání, které lze učinit,
- potřebné softwarového vybavení, pro uskutečnění podání,
- vývoj počtu e-podání v jednotlivých letech.

Individuální kriteria pro zhodnocení současného stavu:

- Ministerstvo financí České republiky
    - vývoj podle jednotlivých měsíců,
    - vývoj podle jednotlivých skupin,
- Česká správa sociálního zabezpečení
    - využívání kvalifikovaných certifikátů a podpisových klíčů ČSSZ,
    - využívání předání e-podání prostřednictvím portálu a záznamových médií,
- Rejstřík trestů Praha
    - srovnání vývoje e-podání s ostatními typy podání,
    - vývoj podání podle žadatelů.

## 5.1 Ministerstvo financí České republiky

Své služby začalo Ministerstvo financí nabízet v roce 2003, jednalo se o 4 typy podání se zaručeným EP. Poté postupně docházelo k rozšiřování služeb. V roce 2004 došlo k navýšení o 4 poskytované služby a v roce 2006 o další 4. Současnosti je tedy možné učinit 12 typů podání se zaručeným EP. Typy podání s jejich postupným zaváděním jsou uvedeny v Tabulka 4.

**Tabulka 4 MF ČR, typy podání a rok zprovoznění služby, zdroj vlastní – upraveno na základě [8]**

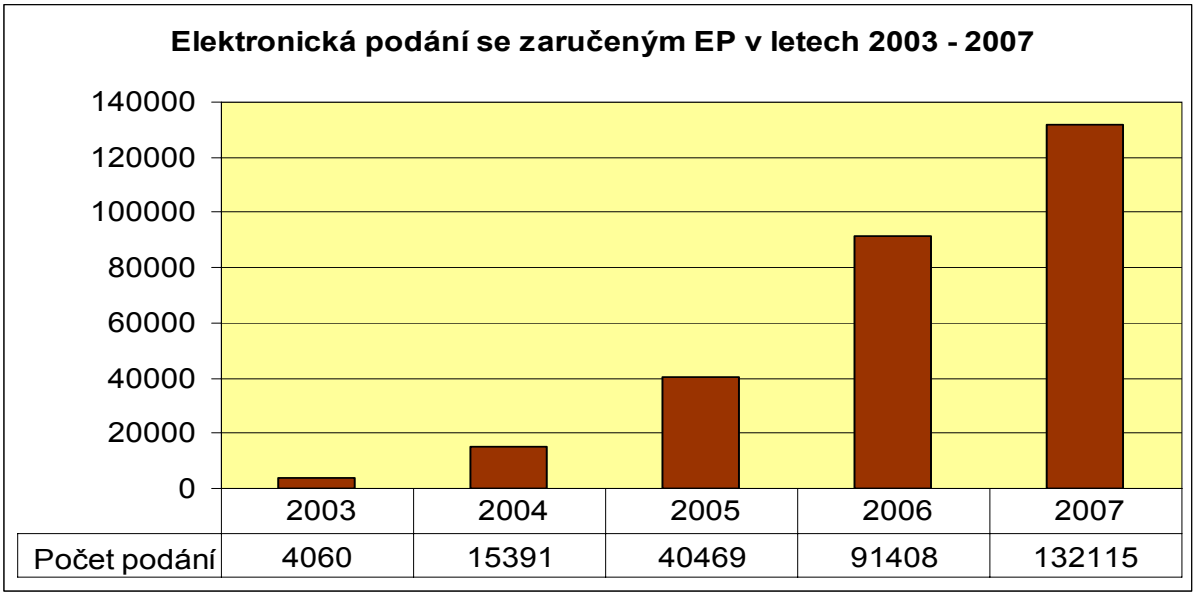
| E-podání | Zavedeno od: |
|---|---|
| Daňové přiznání – daň silniční | 03.2003 |
| Daňové přiznání – daň z nemovitostí | 03.2003 |
| Hlášenky (ozn. dle § 34 zákona o správě daní a poplatků) | 03.2003 |
| Daňové přiznání DPH | 03.2003 |
| Obecné (neformulářové) písemnosti | 10.2003 |
| Souhrnné hlášení VAT Information Exchange System | 05.2004 |
| Daňové přiznání – daň z příjmů fyzických osob (var. A i B) | 06.2004 |
| Daňové přiznání – daň z příjmů právnických osob | 06.2004 |
| Žádost o vrácení přeplatku daně z příjmu fyzických osob | 06.2004 |
| Hlášení platebních zprostředkovatelů | 02.2006 |
| Vyúčtování daně z příjmu fyzických osob ze závislé činnosti a z funkčních požitků | 02.2006 |
| Písemnosti daňového portálu | 06.2006 |

Pro elektronickou komunikaci je třeba počítač s přístupem na internet a softwarové vybavení dle stanovených požadavků, jinak nelze podání uskutečnit. Požadavky na systém se liší podle způsobu práce. Zpracování datového souboru, kontroly podání, podepsání zaručeným elektronickým podpisem a odeslání na Společné technické zařízení správců daně vyžaduje:

- Internet Explorer 6 Service Pack 1 a vyšší (Mozilla 1.6 a vyšší, Firefox 0.8 a vyšší, Netscape 7 a vyšší),
- operační systému Microsoft Windows 2000, Microsoft Windows XP a Knoppix verze 3.6 (Debian Linux),
- prostředí SUN Java (verze 1.5 a vyšší).

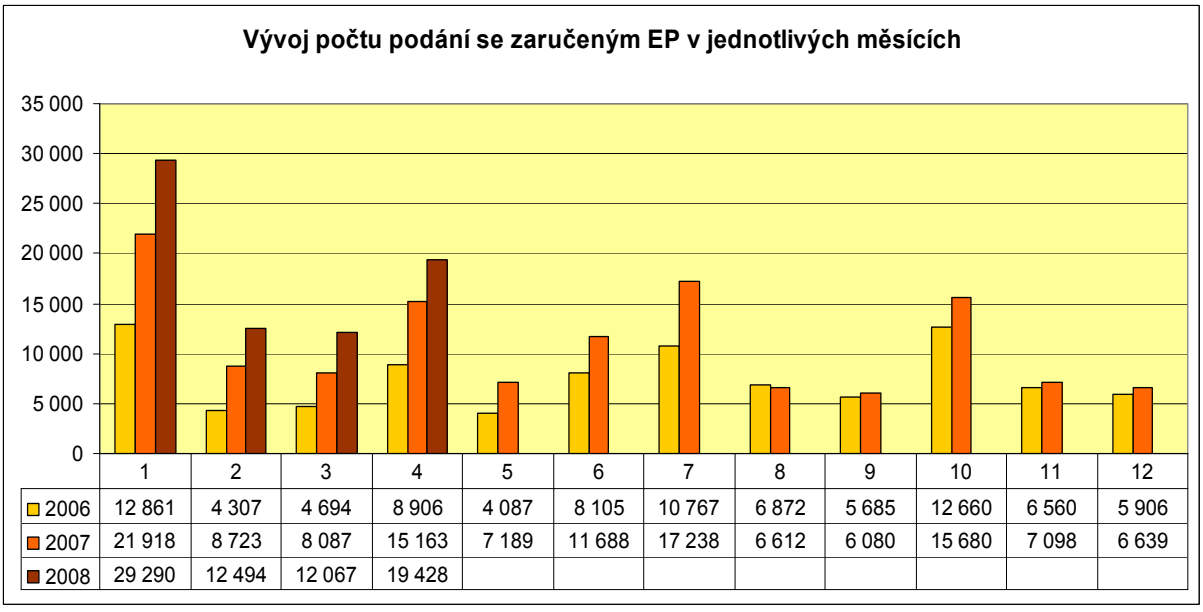
Pro část aplikace sloužící k vytvoření datového souboru vyplněním daňových formulářů a pro instalaci off-line verze celé aplikace lze použít pouze prohlížeč Microsoft Internet Explorer. Podporované jsou tyto verze - Internet Explorer 6 Service Pack 1 a vyšší. Kromě toho je požadováno prostředí Java (jak je již uvedeno výše). Pro správný provoz aplikace e-podání je nutné deaktivovat blokování popup oken. Deaktivaci blokování popup oken je nutno provést před spuštěním aplikace e-podání. Dále je vhodné (nikoliv nezbytné) mít povoleno ukládání cookies.

Vývoj počtu podání v jednotlivých letech je ovlivňován postupným zaváděním nových služeb. Z Graf 4 je patrný nárust podání v roce 2005 a 2006 po prvním rozšíření služeb a další nárust v roce 2007 po druhém rozšíření. Podrobný vývoj jednotlivých e-podání bude znázorněn dále.




**Graf 4 MF ČR, e-podání se zaručeným EP, zdroj vlastní – upraveno na základě [18]**

V Graf 5 je zobrazen vývoj podle jednotlivých měsíců. Největší počet e-podání připadá na měsíc leden, je to období, kdy se setkává nejvíce e-podání (DPH – měsíčně i čtvrtletně, daň z nemovitosti, daň silniční a vyúčtování daně z příjmu fyzických osob ze závislé činnosti a z funkčních požitků). Další nárusty jsou ve čtvrtém, sedmém a desátém měsíci, vždy kdy dojde k opětovnému setkání měsíčního a čtvrtletního DPH.

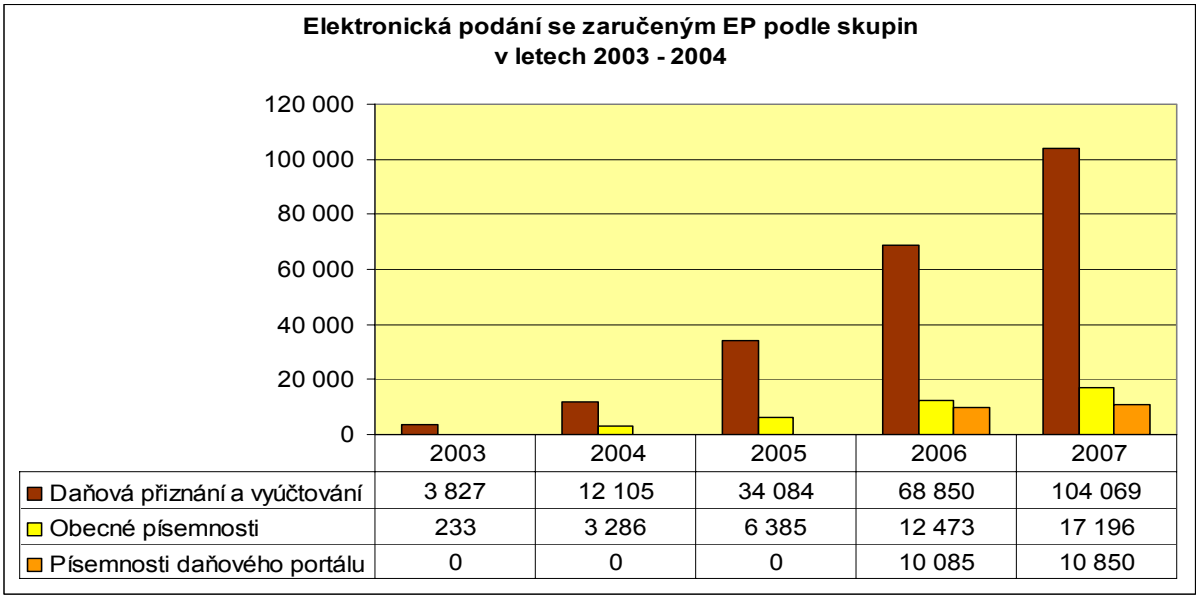



**Graf 5 MF ČR, vývoj počtu podání se zaručeným EP, zdroj vlastní – upraveno na základě [18]**

E- podání lze rozdělit do tří skupin :

- daňové přiznání a vyúčtování,
- obecné písemnosti,
- písemnosti daňového portálu.

Podíl jednotlivých skupin na celkovém počtu podání je vidět v Graf 6. Největší podíl zde má skupina daňová přiznání a vyúčtování. Tento stav je způsoben typem e-podání, která se opakují každoročně, na rozdíl od jiných, která jsou pouze jednorázová a dále e-podáním Daň z přidané hodnoty, které se opakuje čtyřikrát a nebo dvanáctkrát ročně. Tím je způsoben značný nárust e-podání. U skupiny obecné písemnosti není frekvence opakování ničím ovlivněna, jedná se o e-podání podle potřeb klientů. Ve třetí skupině písemnosti daňového portálu se jedná o e-podání jednorázová, tedy využitelná pouze jednou. Vývoj v jednotlivých skupinách a tím i celkový, je ovlivněn frekvencí opakování jednotlivých e-podání.




| | 2003 | 2004 | 2005 | 2006 | 2007 |
|---|---|---|---|---|---|
| Daňová přiznání a vyúčtování | 3 827 | 12 105 | 34 084 | 68 850 | 104 069 |
| Obecné písemnosti | 233 | 3 286 | 6 385 | 12 473 | 17 196 |
| Písemnosti daňového portálu | 0 | 0 | 0 | 10 085 | 10 850 |

**Graf 6 MF ČR, e-podání se zaručeným EP podle jednotlivých skupin, zdroj vlastní – upraveno na základě [18]**

## 5.2 Česká správa sociálního zabezpečení

Česká správa sociálního zabezpečení začala své služby poskytovat od roku 2005. V tomto roce umožnila podávat 2 elektronická podání. K následnému navýšení o 1 službu došlo v roce 2006. Typy podání s jejich postupným zaváděním jsou uvedeny v

**Tabulka 5 ČSSZ, typy podání a rok zprovoznění služby, zdroj vlastní – upraveno na základě [35]**

. V současnosti je tedy možnost podat tři typy e-podání.

**Tabulka 5 ČSSZ, typy podání a rok zprovoznění služby, zdroj vlastní – upraveno na základě [35]**

| E-podání | Zavedeno od: |
|---|---|
| evidenční listy důchodového pojištění (ELDP) | 01.2005 |
| přihlášky a odhlášky zaměstnanců k nemocenskému pojištění (P/O) | 07.2005 |
| přehled o příjmech a výdajích osob samotně výdělečně činných (přehled OSVČ) | 01.2006 |

I přesto, že ČSSZ chtěla nabídku svých služeb rozšířit, nebylo to možné, protože byla odložena účinnost zákona o nemocenském pojištění k 1.1.2009. Od tohoto roku je tedy předpoklad, že dojde k opětovnému navýšení služeb. Mezi nová e-podání by tak měly přibýt:

- evidenční list důchodového pojištění,
- potvrzení o studiu,
- oznámení o nástupu do zaměstnání.

E-podání je na ČSSZ možné doručit dvěma způsoby. První je odeslání přes portál veřejné správy, druhá je doručení na paměťovém médiu. Mezi povolená paměťová média patří disketa 3,5"/1,44 MB nebo CD.

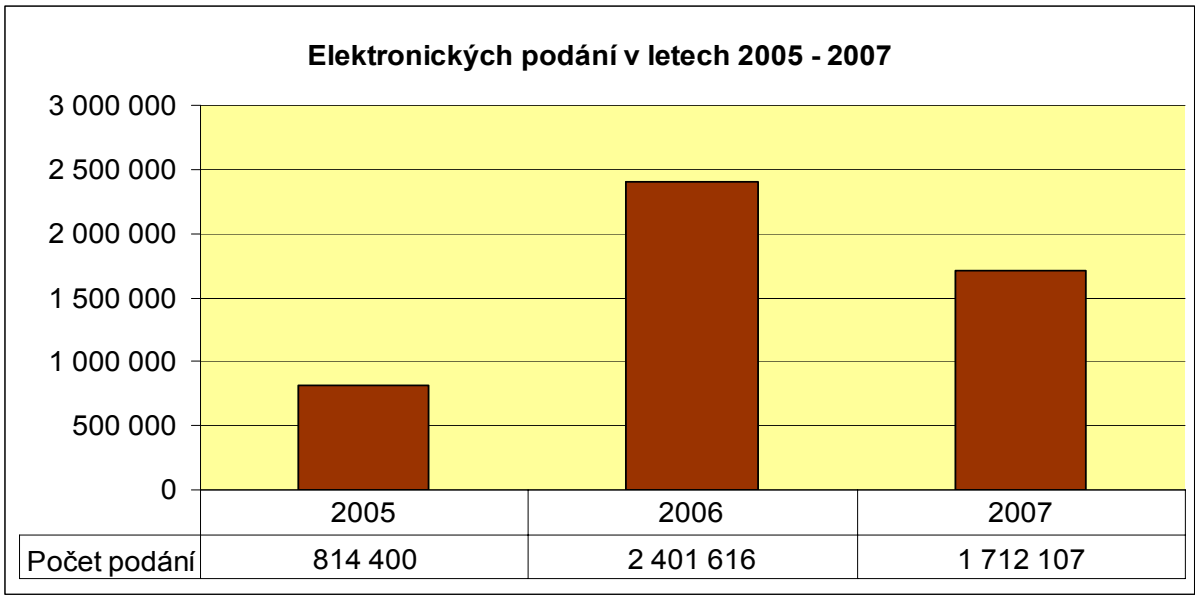
Pro odesílání přes portál jsou dány požadavky na konfiguraci počítače:

- operační systém Windows 2000, XP, 2003, Windows 98 SE, ME,
- internetový prohlížeč Microsoft Internet Explorer 5.5 a vyšší,
- volné místo na HDD - 40 MB volného místa na HDD pro instalaci,
- operační paměť - doporučeno 64 MB (128 MB pro Server).

Pro vyplňování e-tiskopisů je třeba nainstalovat aplikaci 602XML Filler. Podpora je ze strany ČSSZ poskytována pouze tomuto programu, ale lze použít i jiné programy, které vytvoří předepsanou datovou větu, umožní podpis kvalifikovaným certifikátem, zašifrování a odeslání na portál.

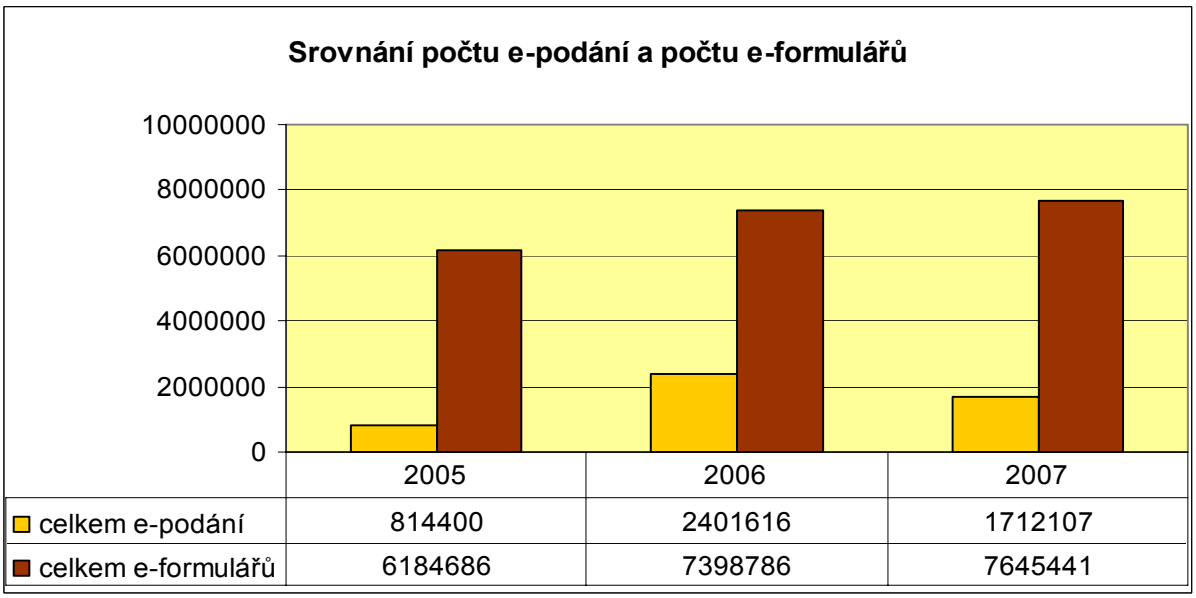
Počet e-podání v jednotlivých letech je znázorněn v Graf 7. Je nutné podotknou, že se nejedná výhradně o podání opatřené zaručeným EP. U ČSSZ je v současné době možné využívat souběžně se zaručeným EP ještě šifrovací certifikát ČSSZ. Ten byl bezplatně nabízen v prvním roce zprovoznění služeb a měl platnost 3 roky a v letošním roce jeho platnost končí. Od 1.2.2006 lze využívat pouze kvalifikovaný certifikát. U poskytnutých údajů o e-podání nejsou tyto dvě možnosti nijak rozlišeny. Aby mohl být znázorněn vývoj e-podání, je v grafu kvalifikovaný

certifikát postaven naroveň šifrovacímu certifikátu ČSSZ, protože je zde předpoklad, že klienti po skončení platnosti šifrovacího certifikátu budou využívat kvalifikovaný certifikát.



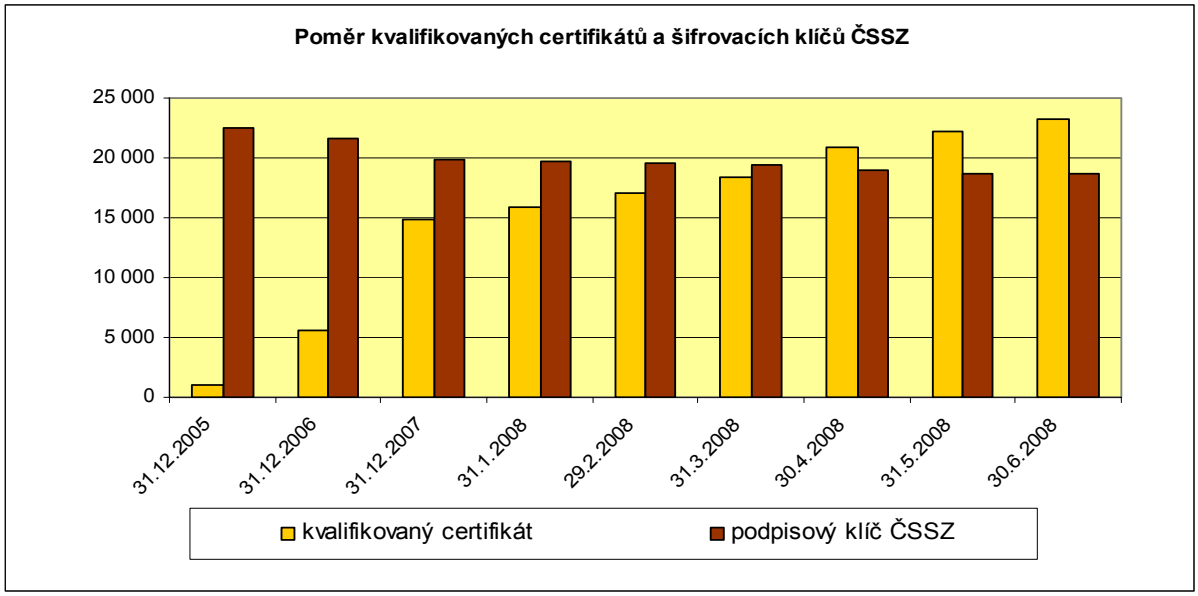

**Graf 7 ČSSZ, e-podání, zdroj vlastní – upraveno na základě [3]**

Z Graf 7 je zřejmé, že v roce 2007 došlo k více než desetiprocentnímu poklesu oproti roku 2006. Tato situace je způsobena tím, že v jednom podání může být zasláno více e-formulářů. Pokud tedy hovoříme o e-podáních, pak jejich počet poklesl. K jakému zkreslení může dojít je ukázáno na následujícím Graf 8. V roce 2007 je zde zaznamenán pokles e-podání a zároveň nárust e-formulářů.



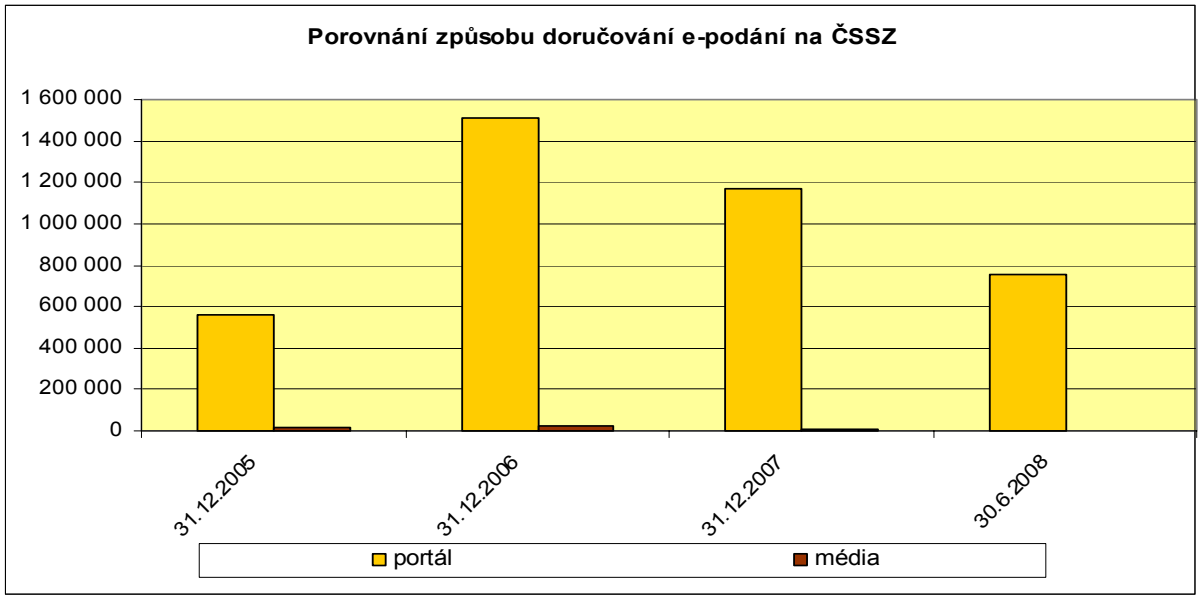

**Graf 8 ČSSZ, srovnání počtu podání a počtu e-formulářů, zdroj vlastní – upraveno na základě [3]**

Porovnání využívání kvalifikovaných certifikátů a šifrovacích certifikátů ČSSZ je v Graf 9. Z počátku zavedení služeb je vidět naprostá převaha šifrovacích klíčů ČSSZ. Na počátku letošního roku začínají převažovat kvalifikované certifikáty, což je způsobeno ukončením platnosti šifrovacích certifikátů ke konci letošního roku. Využití celé doby platnosti šifrovacího certifikátu bylo pro klienty výhodné, protože jeho pořízení bylo bezplatné.




**Graf 9 Poměr kvalifikovaných certifikátů a šifrovacích klíčů ČSSZ, zdroj vlastní – upraveno na základě [3]**

V následujícím Graf 10 je znázorněn poměr způsobu doručování e-podání na ČSSZ. Klienti mají dvě možnosti, jedna je vytvoření datové zprávy, její podepsání a odeslání přes portál, druhá je vytvoření datové zprávy, její podepsání a nahrání na záznamové médium a doručení na ČSSZ podle působnosti. Graf znázorňuje převahu využívání portálu, při kterém klientům odpadá doručování přenosného média na pobočku a nedochází k časovým prodlevám spojeným s cestou a v některých případech i čekáním, než na klienta přijde řada.




**Graf 10 Porovnání způsobu doručování na ČSSZ, zdroj vlastní – upraveno na základě [3]**

## 5.3 Rejstřík trestů Praha

Služby Rejstříku trestů jsou nabízeny od poloviny roku 2006. Pro fyzické osoby jsou k dispozici následující druhy e-podání:

- žádost o informativní výpis z rejstříku trestů,
- žádost o výpis z rejstříku trestů,
- žádost o nahlédnutí do opisu z rejstříku trestů,
- žádost o informaci, kdy a komu byly vydány výpisy a opisy.

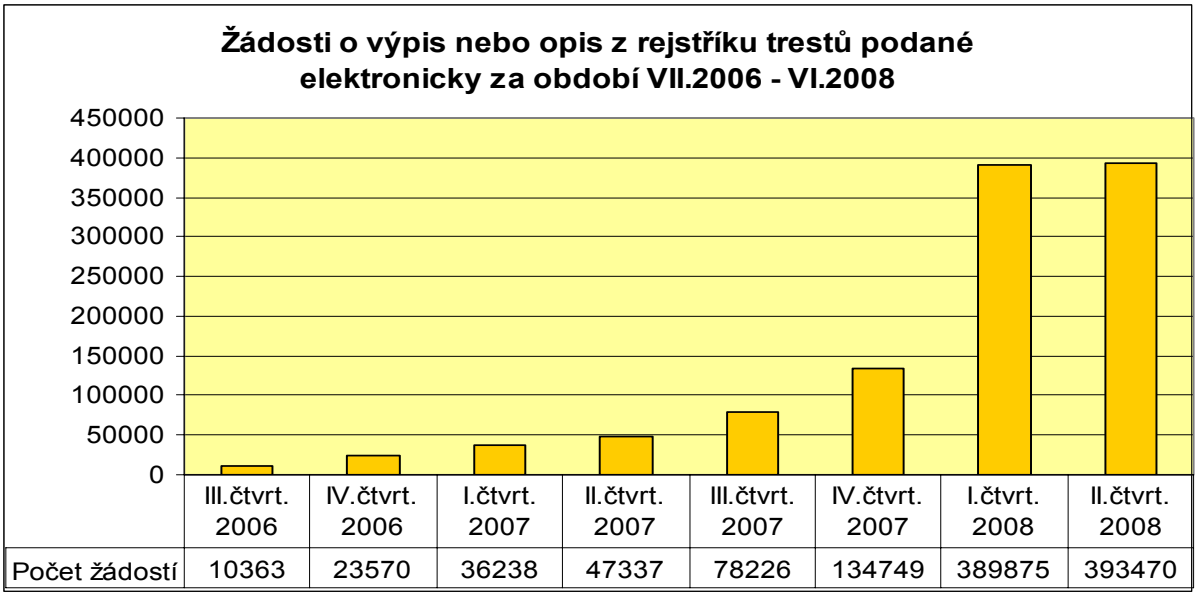
Od 1.7.2008 jsou služby rozšířeny i pro orgány veřejné moci a ty mají možnost využít následující e-podání:

- žádost o výpis z rejstříku trestů,
- žádost o opis z rejstříku trestů.

Komunikujeme-li s RT přes webový formulář pomocí internetového prohlížeče není třeba specielní software, postačí připojení na internet a internetový prohlížeč. Pro komunikaci prostřednictvím klienta webové služby je zapotřebí aplikace, která se spojuje s aplikací rejstříku trestů.

**V Graf 11 je znázorněn vývoj počtu e-podání. Je nutné podotknout, že se nejedná výhradně o e-podání opatřená zaručeným EP. Část e-podání je opatřená elektronickou značkou založenou na kvalifikovaném systémovém certifikátu. RT Praha tyto údaje nerozlišuje, protože se jedná pouze o rozdílné způsoby komunikace. Jelikož je služba nabízena velmi krátkou dobu byl pro lepší přehlednost znázorněn vývoj po jednotlivých čtvrtletích. Z grafu je viditelný strmý nárust počtu e-podání v roce 2008. Jedná se o období, kdy byla spuštěna služba Czech POINT a dále byly zprovozněny další dálkové přístupy. Podrobný graf vývoje počtu e-podání po jednotlivých měsících je znázorněn v**

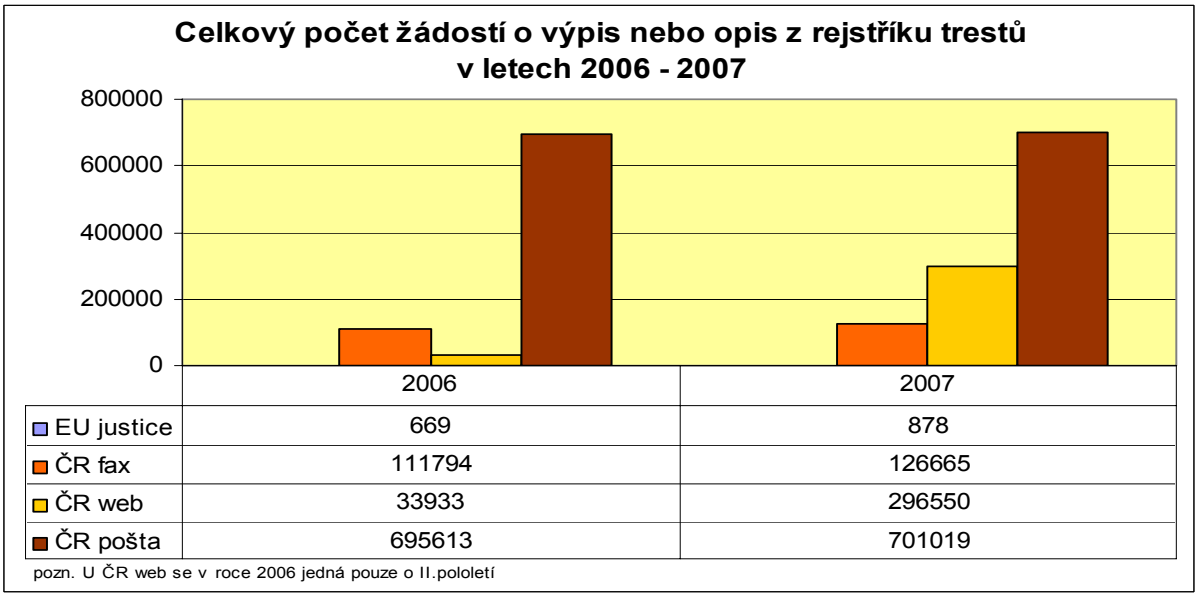
Příloha 4.




| | III.čtvrt. 2006 | IV.čtvrt. 2006 | I.čtvrt. 2007 | II.čtvrt. 2007 | III.čtvrt. 2007 | IV.čtvrt. 2007 | I.čtvrt. 2008 | II.čtvrt. 2008 |
|---|---|---|---|---|---|---|---|---|
| Počet žádostí | 10363 | 23570 | 36238 | 47337 | 78226 | 134749 | 389875 | 393470 |

**Graf 11 Žádosti o výpis nebo opis z RT podané elektronicky, zdroj vlastní – upraveno na základě [15]**

Jaký je podíl elektronicky podaných žádostí oproti všem žádostem, které byly doručeny na RT je v následujícím Graf 12. V roce 2006 tvoří jen velmi malou část, příčinou je také spuštění služby až ve druhém pololetí, ale v roce 2007 již e-podání tvoří více než čtvrtinu všech písemností. Pro zhodnocení I. pololetí 2008 nebyla data poskytnuta.



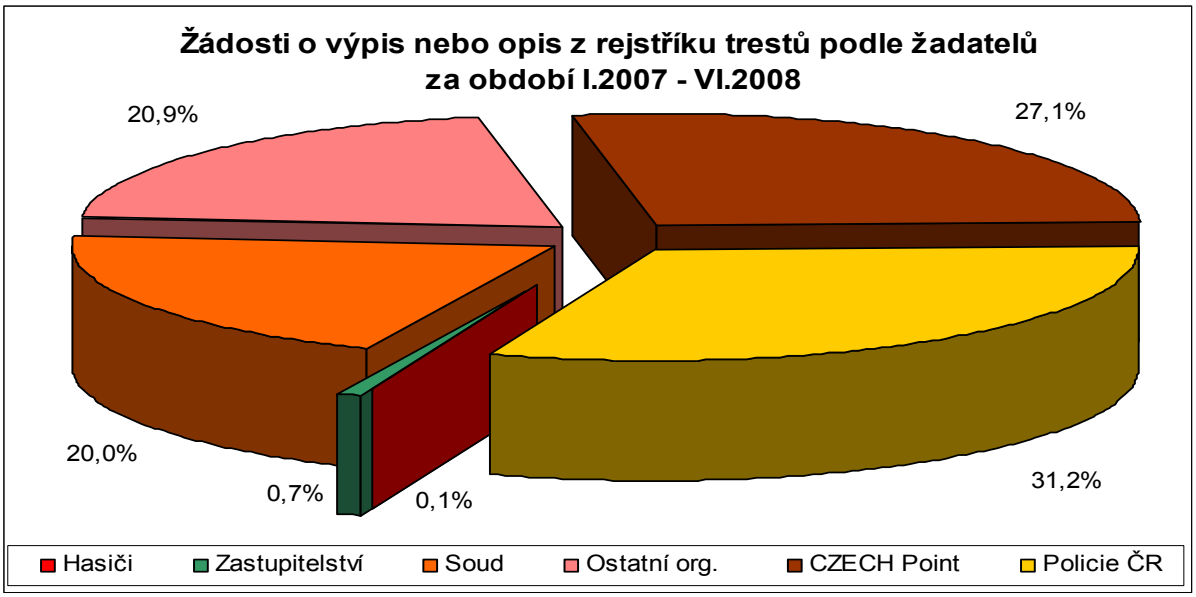

| | 2006 | 2007 |
|---|---|---|
| EU justice | 669 | 878 |
| ČR fax | 111794 | 126665 |
| ČR web | 33933 | 296550 |
| ČR pošta | 695613 | 701019 |

pozn. U ČR web se v roce 2006 jedná pouze o II.pololetí

**Graf 12 Celkový počet žádostí o výpis nebo opis z RT, zdroj vlastní – upraveno na základě [15]**

Které orgány státní správy mají největší podíl na elektronicky podaných žádostech o výpis nebo opis z RT za období leden 2007 až červen 2008 je vidět v Graf 13. Největší podíl, téměř třicetiprocentní, patří Policii ČR, za kterou následuje služba CZECH Point a poté soudy

s dvaceti procenty. Další dvacetiprocentní podíl patří ostatním organizacím, jako jsou např. krajské úřady, ministerstva, Národní bezpečnostní úřad, živnostenské úřady atd..




**Graf 13 Žádosti o výpis nebo opis z RT podle žadatelů, zdroj vlastní – upraveno na základě [15]**

## 5.4 Shrnutí

Možnosti podat e-podání se různí podle typu orgánů státní správy. Ministerstvo financí ČR většinu svých služeb poskytuje jak v papírové, tak v elektronické podobě. Elektronicky nelze ještě např. podat daň dědickou, daň darovací, daň z převodu nemovitostí. Brání tomu technické důvody, respektive nemožnost vložit potřebné přílohy. Přes veškerou snahu rozšiřovat nabízené služby je poměr e-podání ve srovnání s klasickými velmi nízký. Jako příklad je uvedeno Finanční ředitelství v Brně, kde se elektronická podání (se zaručeným i bez zaručeného EP) podílela na celkovém počtu všech podání v roce 2006 0,73 % a v roce 2007 1,01 %.

Česká správa sociálního zabezpečení má velmi nízký počet druhů podání, které je možné provést elektronicky. Jedním z důvodů je zde pomalá legislativa, protože i přes snahu ČSSZ rozšířit své služby, se toto stává nemožným. I přesto, že nedochází k navyšování nových služeb, jsou stávající služby stále více využívány. Dle údajů ČSSZ využilo v I. pololetí letošního roku možnosti elektronicky podávat dokumenty více než 71,5 % organizací s více než 25 zaměstnanci.

Rejstřík trestů Praha nabízí své služby v elektronické i klasické podobě. Jejich využívání postupně narůstá. Zatím co se v roce 2006, (zavedení služby v druhé polovině roku), e-podání na celkovém počtu všech podání podílela necelými 4 %, v roce 2007 to již bylo již více než 25 %. Při vysokém nárustu na počátku letošního roku a při dalším předpokládaném v jeho průběhu může dosáhnout ke konci roku 50 %.

Specielní softwarové vybavení nevyžaduje ani jeden z hodnocených orgánů státní správy. Veškerý potřebný software je k dispozici u jednotlivých poskytovatelů a je možné ho získat na jejich internetových stránkách. Problém nastává spíše ve správném nastavení počítače, aby mohly být dané služby využívány. To je mnohdy složitá záležitost a ne všichni uživatelé jsou schopni jí porozumět.

Roční nárusty e-podání jsou zřejmé u všech sledovaných orgánů státní správy. Nárust počtu jednotlivých e-podání se liší podle možnosti jejich využití. Některá jsou jednorázovou záležitostí (např. u MFČR Žádost o zřízení/zrušení daňové informační schránky), jiná se opakují pouze jedenkrát ročně (např. u MF ČR Daň z nemovitosti) a další jsou využívány dle potřeby (např. u ČSSZ Přihlášky a odhlášky zaměstnanců k nemocenskému pojištění).

## 5.5 Výhody a nevýhody využití elektronických podání

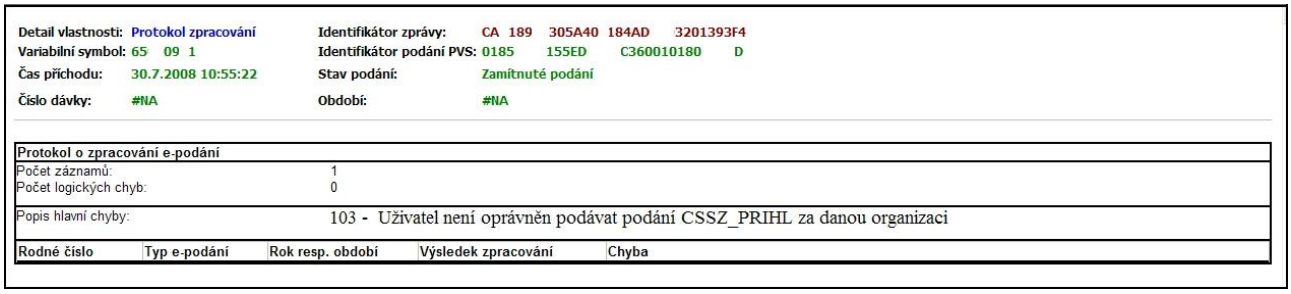
Jednou z velkých výhod je dostupnost služby 24 hodin denně 7 dní v týdnu. Klienti nejsou tedy omezeni pracovní dobou úřadů, nedochází ani k časovým ztrátám, kdy byl klient nucen osobně dojít na úřad a nebo na poštu, pokud chtěl doručit klasické ruční podání. Okamžitá odezva umožňuje ověřit, zda bylo e-podání doručeno a nebo zamítnuto. Klient tedy, pokud to jde, může chybné podání okamžitě opravit a nebo zpracovat nové. Při vyplňování e-podání jsou využívány interaktivní inteligentní formuláře se zabudovanými kontrolními prvky, které neumožní při závažných chybách odeslání formuláře (např. nevyplnění povinných údajů). Další výhodou je i osvobození od poplatku dle § 8, odst. 2 zákona číslo 634/2004 Sb. správní řád. Tato skutečnost však není mezi klienty moc známa.

Výhodou pro orgány státní moci je jednoznačné určení a ověření identity podepisující osoby, dále integrity dat, tedy nedošlo-li po podepsání datové zprávy k případným změnám. A v neposlední řadě jde i o nepopiratelnost, klient tedy nemůže popřít, že dané e-podání podepsal.

Nevýhodou je, že získání elektronického podpisu může být pro mnohé klienty velmi složitou záležitostí. Další komplikace mohou nastat při nastavení počítače, aby mohlo docházet k odesílání e-podání. Mnozí klienti této problematice nerozumí a je to tedy pro ně velmi složitá záležitost. Dále při chybě, která je zjištěná v e-podání, které obsahuje více e-formulářů, nedojde k zamítnutí pouze formuláře ve kterém se vyskytuje chyba, ale k zamítnutí všech formulářů. Paradoxně tak může docházet k navyšování počtu ručních podání, protože klient často není schopen chybu nalézt a je pro něho jednodušší formuláře vytisknout a doručit na pobočku. Pro fyzickou osobu,

která nepodniká, je možnost využívat e-podání prakticky nulová a to i přes nízkou cenu certifikátu 190,- Kč.

Pro orgány státní správy jsou nevýhodou chyby, které vznikají při vyplňování e-formulářů, při vícenásobném odeslání nebo při duplicitě dat. K dalším chybám může např. docházet, když odesílající není oprávněn podat e-podání. Ukázka takového zamítnutí e-podání u ČSSZ je na následujícím Obrázek 11.



| | | | |
|---|---|---|---|
| Detail vlastnosti: | Protokol zpracování | Identifikátor zprávy: | CA 189 305A40 184AD 3201393F4 |
| Variabilní symbol: | 65 09 1 | Identifikátor podání PVS: | 0185 155ED C360010180 D |
| Čas příchodu: | 30.7.2008 10:55:22 | Stav podání: | Zamítnuté podání |
| Číslo dávky: | #NA | Období: | #NA |

| Protokol o zpracování e-podání | | | | |
|---|---|---|---|---|
| Počet záznamů: 1<br>Počet logických chyb: 0 | | | | |
| Popis hlavní chyby: | 103 - Uživatel není oprávněn podávat podání CSSZ_PRIHL za danou organizaci | | | |
| Rodné číslo | Typ e-podání | Rok resp. období | Výsledek zpracování | Chyba |

**Obrázek 11 Chybové hlášení o nepřijetí e-podání u ČSSZ, zdroj vlastní – upraveno na základě [35]**

## 5.6 Možnosti dalšího využití

Mezi možnosti využití elektronického podpisu u orgánů státní správy patří komunikace Rejstříku trestů Praha s Network Judicia Register , což je elektronická síť trestních rejstříků členských států Evropské unie. Nepoužívá se zde přímo kvalifikovaný elektronický podpis platný a používaný na území České republiky, ale jeho obdoba, na které se připojené země dohodly, včetně specielního šifrovacího software. Pro zabezpečenou komunikaci s okolními státy je využívána evropská síť S-TESTA, což je obdoba sítě Govnet využívané v rámci státní správy České republiky, ale na celoevropské úrovni. Prozatím jsou touto sítí propojeny Německo, Francie, Belgie, Španělsko, Lucembursko a nově také Česká republika, která poskytla/využila první služby v listopadu 2007. Komise Evropské unie předpokládá, že do 3-5 let budou napojeny i rejstříky trestů ostatních zemí, které si budou vzájemně poskytovat informace o odsouzených osobách (doposud tomu tak bylo v papírové podobě). [27]

Možnost dalšího využití je závislá na schválení Zákona o elektronických úkonech, osobních číslech a autorizovaného konverzi dokumentů a jeho využití při postupech podle správního řádu. Ten by měl upravit komunikaci mezi občany a úřady a úřady navzájem. Účinnost zákona je plánována k 1.7.2009. Základní změny, které má zákon přinést jsou následující [28]:

- jednotný systém pro elektronické doručování dokumentů,
- doručování prostřednictvím datových schránek,
- autorizovaná konverze dokumentů.

Předpokládá se zde zavedení datových schránek s jednoznačnou a nezaměnitelnou adresou, prostřednictvím kterých bude probíhat komunikace s úřady. Pro úřady a právnické osoby je komunikace prostřednictvím datové schránky povinností, občan může volit mezi touto a písemnou komunikací. Využívání schránek má ušetřit čas a peníze a také nenáročné uživatelské prostředí má přispět k rozšířenému využívání.

Autorizovanou konverzí dokumentů se zde rozumí úplné převedení dokumentu v elektronické podobě do podoby listinné a naopak. Takto vzniklý dokument má stejné právní účinky jako ověřená kopie dokumentu a provádět ho mohou pouze pověřené subjekty.

Využitím datových schránek se zjednoduší doručování pro správní orgány, zejména pokud jde o rychlost a ekonomickou stránku. Zásadní je doba určení okamžiku doručení, protože se jedná o významnou právní skutečnost a jsou možné dva způsoby [28]:

- dokument, který byl dodán do datové schránky, je doručen okamžikem, kdy se do datové schránky přihlásí osoba, která má s ohledem na rozsah svého oprávnění přístup k dodanému dokumentu,
- nepřihlásí-li se do datové schránky výše uvedená osoba ve lhůtě 10 dnů ode dne, kdy byl dokument dodán do datové schránky, považuje se tento dokument za doručený posledním dnem této lhůty (jsou možné i výjimky jako např. v trestním řízení).

# Závěr

Využití elektronického podpisu při komunikaci občanů nebo organizací s orgány státní správy je v celkovém pohledu téměř mizivé. Převážně se jedná o komunikaci jednostrannou a to od občanů a organizací směrem ke státní správě, v opačné rovině komunikace takřka není, protože tomu brání legislativní překážky. Přesto se i zde již dají najít výjimky a to právě v podobě orgánů státní správy, které přijímají elektronická podání.

Ve své práci jsem se zaměřila na popsání a vysvětlení klíčových pojmů souvisejících s elektronickým podpisem, ukázala jsem postup, jak je možné získat kvalifikovaný elektronický podpis založený na kvalifikovaném certifikátu, který je jako jediný akceptován orgány státní správy. Zabývala jsem se legislativou, tedy vývojem právních norem a zákonů. Pro ucelený přehled jsou zde uvedeny všechny normy a předpisy, i když některé v současné době již neplatí. Dále byly vybrány certifikační autority, které vydávají kvalifikované certifikáty a podle předem stanovených kritérií byly hodnoceny nabízené služby.

Aby mohly být zhodnoceny možnosti pro e-podání, byly zmapovány internetové stránky orgánů státní správy a zjištěny možnosti, které jsou nabízeny. Lze je rozdělit do tří kategorií z nichž u první je uvedena adresa e-podatelny nebo adresa pro příjem datových zpráv, ale další podmínky nejsou blíže specifikovány. U druhé kategorie je uvedena adresa e-podately pro příjem datových zpráv, blíže specifikovány podmínky pro jejich přijímání, stanoveno, které druhy datových zpráv musí být podepsány zaručeným EP a vyjmenovány certifikační autority, které akceptují. Třetí kategorii tvoří orgány, které přijímají e-podání „hromadně“ a to buď přímo na svých internetových stránkách v e-podalně a nebo je zde zveřejněn odkaz na stránky, kde je možné takové podání učinit. K podpisu těchto podání je třeba EP založený na kvalifikovaném certifikátu vydaný akreditovaným poskytovatelem certifikačních služeb. Seznamy poskytovatelů, kteří jsou akceptováni, jsou uvedeny na těchto stránkách. Spadají sem i e-podání druhé kategorie.

Pro zhodnocení současného stavu, podle předem zvolených kritérií, byly vybrány orgány státní správy ze třetí kategorie. Hodnoceny byly druhy nabízených služeb, softwarové vybavení a vývoj počtu e-podání. Rozšiřování služeb brání legislativní překážky, některé subjekty mají připravenu novou nabídku služeb, ale z tohoto důvodu ji nemohou rozšiřovat. Pro vyhotovení a odeslání e-podání není třeba specielního softwarového vybavení, problém je spíše ve správném nastavení počítače, aby mohly být dané služby využívány. To je mnohdy složitá záležitost a ne všichni uživatelé jsou schopni jí porozumět. Roční nárusty e-podání závisí na možnosti jejich využití. Některá jsou jednorázovou záležitostí, jiná se opakují pouze jedenkrát ročně a další jsou využívány

dle potřeby. V závěru byly zhodnoceny výhody a nevýhody elektronických podání. Lze říci, že elektronický podpis předběhl dobu. Můžeme vytvářet datové zprávy, podepisovat je a odesílat, ale stát nám nevytváří dostatečné pobídky pro jeho větší využívání.

# Seznam literatury a použitých zdrojů


[1] *Archiv stránek bývalého Ministerstva informatiky* [online]. [cit. 2008-01-10]. Dostupný z WWW: <http://www.mvcr.cz/micr/default.htm>.

[2] BOSÁKOVÁ, Dagmar 2002, et al. *Elektronický podpis přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů*. 1. vyd. Olomouc : Nakladatelství ANAG, 2002. 141 s. ISBN 80-7263-125-X.

[3] BURANOVÁ, Jana. *Interní materiály elektronického podání*. Česká správa sociálního zabezpečení Praha Praha, [cit. 2008-07-14].

[4] *Celní správa* [online]. 2005 [cit. 2008-07-14]. Dostupný z WWW: <http://www.cs.mfcr.cz/cmsgrc/>.

[5] *Centrální ohlašovna* [online]. 2005-2008 [cit. 2008-07-15]. Dostupný z WWW: <http://www.centralniohlasovna.cz/co-web/web>.

[6] *Česká daňová správa* [online]. 2006 [cit. 2008-07-14]. Dostupný z WWW: <http://cds.mfcr.cz/cps/rde/xchg/cds/xsl/329.html>.

[7] *Český úřad zeměměřičský a katastrální* [online]. [cit. 2008-07-20]. Dostupný z WWW: <http://www.cuzk.cz/Dokument.aspx?PRARESKOD=10&Akce=GEN:UVOD>.

[8] *Daňový portál* [online]. 2006 [cit. 2008-07-14]. Dostupný z WWW: <http://adisspr.mfcr.cz/adistc/adis/idpr_pub/dpr/uvod.faces>.

[9] DOSTÁLEK, Libor, VOHNOUTOVÁ, Marta 2006, *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*. 1. vyd. Brno : Nakladatelství Computer Press, 2006. 534 s. ISBN 80-251-0828-7.

[10] *eIdentity a.s.* [online]. 2005 [cit. 2008-01-08]. Dostupný z WWW: <https://www.eidentity.cz/app>.

[11] *Generální ředitelství cel* [online]. 2005 [cit. 2008-07-14]. Dostupný z WWW: <http://www.cs.mfcr.cz/>.

[12] *Integrovaný portál MPSV* [online]. 2002-2008 [cit. 2008-07-16]. Dostupný z WWW: <http://portal.mpsv.cz/sprava>.

[13] *Justice.cz* [online]. [cit. 2008-07-14]. Dostupný z WWW: <http://portal.justice.cz/uvod/justice.aspx>.

[14] KOUKOLÍK, Zbyněk. *Interní materiály vydávání kvalifikovaných certifikátů*. Ministerstvo vnitra České republiky, [cit. 2008-07-14].

[15] KRÁTKORUKÝ, Zdeněk. *Interní materiály elektronického podání*. Rejstřík trestů Praha, [cit. 2008-07-14].

[16] *Ministerstvo práce a sociálních věcí* [online]. [cit. 2008-07-16]. Dostupný z WWW: <http://www.mpsv.cz/cs/>.

[17] *Ministerstvo vnitra* [online]. 2006 [cit. 2008-01-08]. Dostupný z WWW: <http://www.mvcr.cz/>.

[18] MRÁČKOVÁ, Milena. *Interní materiály elektronického podání*. Ministerstvo financí České republiky, [cit. 2008-07-14].

[19] Nařízení vlády č. 304/2001 ze dne 25. července 2001 kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu). In *Sbírka zákonů České republiky*. 2001, částka 117, s. 7078. Dostupný také z WWW: <http://aplikace.mvcr.cz/sbirka/2000/sb117-00.pdf>. Platnost ukončena nařízením vlády č. 495/2004 Sb.

[20] Nařízení vlády č. 495/2004 ze dne 25. srpna 2004 kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) ve znění pozdějších předpisů. In *Sbírka zákonů České republiky*. 2004, částka 171, s. 9670-9671. Dostupný také z WWW: <http://aplikace.mvcr.cz/sbirka/2004/sb171-04.pdf>.

[21] *Návrh zákona o elektronických úkonech* [online]. 2008 [cit. 2008-08-15]. Dostupný z WWW: <http://www.langer.cz/egon/data/docisss/doc/eGAct.doc>.

[22] NOVOTNÝ, Zbyněk. Novela zákona o elektronickém podpisu [online]. [cit. 2008-01-08]. Dostupný z WWW: <http://www.zbyneknovotny.cz/monitoring/a.asp?a=2002711&db=110>

[23] Oznámení Ministerstva informatiky ze dne 2006 Přehled udělených akreditací k působení jako akreditovaný poskytovatel certifikačních služeb. In Věstník *Ministerstva informatiky*. 2006, částka 2, s. 2. Dostupný také z WWW: <http://www.mvcr.cz/micr/files/3153/mi_v2006c2_20060908.pdf>.

[24] *PostSignum QCA* [online]. 2005 [cit. 2008-01-08]. Dostupný z WWW: <http://qca.postsignum.cz/>.

[25] *Právní rádce* [online]. 1996-2008 [cit.2008-01-20]. Dostupný z WWW: <http://pravniradce.ihned.cz/>.

[26] *První certifikační autorita, a.s.* [online]. 2000-2006 [cit. 2008-01-08]. Dostupný z WWW: <http://www.ica.cz/home_cs/>.

[27] *Rejstřík trestů* [online]. [cit. 2008-07-14]. Dostupný z WWW: <http://portal.justice.cz/soud/soud.aspx?o=203&j=213&k=2027>.

[28] *Revoluce ve veřejné správě* [online]. 2008 [cit. 2008-08-15]. Dostupný z WWW: <http://www.mvcr.cz/clanek/revoluce-ve-verejne-sprave.aspx>.

[29] *Saferinternet* [online]. [cit. 2008-07-25]. Dostupný z WWW: <http://www.saferinternet.cz/articles.asp?idk=1&ida=399>.

[30] Sdělení úřadu ze dne 15.dubna 2002 Přehled poskytovatelů certifikačních služeb vydávajících kvalifikované certifikáty. In Věstník *Úřadu pro ochranu osobních údajů*. 2002, částka 16, s. 1430.

[31] *SkyNet, a.s.* [online]. 2008 [cit. 2008-06-25]. Dostupný z WWW: <http://www.pgp.cz/index.php?l=cz&p=6&r=5/>.

[32] SMEJKAL, Vladimír. Elektronický podpis [online]. [cit. 2008-01-08]. Dostupný z WWW: <http://moderniobec.ihned.cz/1-10002840-22241485-C00000_detail-4c>

[33] SMEJKAL, Vladimír. Elektronický podpis v praxi [online]. [cit. 2008-01-08]. Dostupný z WWW: <http://pravniradce.ihned.cz/1-10078240-10025905-F00000_detail-a4>

[34] SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 1999/93/EC ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy. In *Ústřední věstník Evropské unie*. 2000, částka 13/sv. 24, s. 239-248. Dostupný také z WWW:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:24:31999L0093:CS:PDF>

[35] *Správa sociálního zabezpečení* [online]. [cit. 2008-07-14]. Dostupný z WWW: <http://www.cssz.cz/cz/novinky/>.

[36] ŠKORPIL, Martin. *Interní materiály vydávání kvalifikovaných certifikátů*. První certifikační autorita a.s., [cit. 2008-07-14].

[37] ŠLANCAR, Martin. *Interní materiály vydávání kvalifikovaných certifikátů*. Česká pošta a.s., [cit. 2008-07-14].

[38] *VersaSystems* [online]. 1998-2008 [cit. 2008-07-16]. Dostupný z WWW: <http://www.versasys.cz/index.php?node=51>.

[39] *Vrchní státní zastupitelství v Praze* [online]. [cit. 2008-07-14]. Dostupný z WWW: <http://portal.justice.cz/soud/soud.aspx?o=205&j=215&k=2046>.

[40] Vyhláška č. 496/2004 ze dne 29. července 2004 o elektronických podatelnách. In *Sbírka zákonů České republiky*. 2004, částka 171, s. 9672-9676. Dostupný také z WWW: <http://aplikace.mvcr.cz/sbirka/2004/sb171-04.pdf>.

[41] Vyhláška č. 378/2006 ze dne 19. července 2006 o postupech kvalifikovaných poskytovatelů certifikačních služeb, o požadavcích na nástroje elektronického podpisu a o požadavcích na ochranu dat pro vytváření elektronických značek (vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb). In *Sbírka zákonů České republiky*. 2006, částka 120, s. 4970-4987. Dostupný také z WWW: <http://aplikace.mvcr.cz/sbirka/2006/sb120-06.pdf>.

[42] Vyhláška Úřadu pro ochranu osobních údajů č. 366/2001 ze dne 3. října 2001 o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu. In *Sbírka zákonů České republiky*. 2001, částka 138, s. 7878-7883. Dostupný také z WWW: <http://aplikace.mvcr.cz/sbirka/2001/sb138-01.pdf>. Platnost ukončena vyhláškou č. 378/2006 Sb.

[43] Zákon č. 227/2000 ze dne 29. června 2000 o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu). In *Sbírka zákonů České republiky*. 2000, částka 68, s. 3290-3297. Dostupný také z WWW: <http://aplikace.mvcr.cz/sbirka/2000/sb068-00.pdf>.

[44] Zákon č. 226/2002 ze dne 9. května 2002, kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, zákon č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů, zákon číslo 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů, zákon číslo 71/1967 Sb., o správním řízení (správní řád), ve znění pozdějších předpisů, a zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu). In *Sbírka zákonů České republiky*. 2002, částka 87, s. 5034-5036. Dostupný také WWW: <http://aplikace.mvcr.cz/sbirka/2002/sb087-02.pdf>.

[45] Zákon č. 517/2002 ze dne 14.listopadu 2002, kterým se provádějí některá opatření v soustavě ústředních orgánů státní správy a mění některé zákony. In *Sbírka zákonů České republiky*. 2002, částka 179, s. 10149-10152. Dostupný také z WWW:<http://aplikace.mvcr.cz/sbirka/2002/sb179-02.pdf>.

[46] Zákon č. 440/2004 ze dne 24. června 2004, kterým se mění zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu),

ve znění pozdějších předpisů. In *Sbírka zákonů České republiky*. 2004, částka 144, s. 8363-8373. Dostupný také z WWW: <http://aplikace.mvcr.cz/sbirka/2004/sb144-04.pdf>.

[47] Zákon č. 486/2004 úplné znění zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), jak vyplývá z pozdějších změn. In *Sbírka zákonů České republiky*. 2004, částka 167, s. 9503-9514. Dostupný také z WWW: <http://aplikace.mvcr.cz/sbirka/2004/sb167-04.pdf>.

[48] Zákon č. 525/2004 předseda vlády vyhlašuje úplné znění zákona č. 101/2000Sb., o ochraně osobních údajů a o změně některých zákonů, jak vyplývá ze změn provedených zákonem č. 227/2000 Sb, zákonem č. 177/2001 Sb., zákonem č. 450/2001 Sb., zákonem č. 107/2002 Sb., zákonem č. 309/2002 Sb., zákonem č. 310/2002 Sb., zákonem č. 517/2002 Sb., zákonem č. 439/2004 Sb. a zákonem č. 480/2004 Sb. ZÁKON o ochraně osobních údajů. In *Sbírka zákonů České republiky*. 2004, částka 180, s. 9967-9981. Dostupný také z WWW: <http://aplikace.mvcr.cz/sbirka/2004/sb180-04.pdf>.

[49] Zákon č. 110/2007 ze dne 19.dubna 2007 o některých opatřeních v soustavě ústředních orgánů státní správy, souvisejících se zrušením Ministerstva informatiky a o změně některých zákonů. In *Sbírka zákonů České republiky*. 2007, částka 41, s. 1335-1338. Dostupný také z WWW: <http://aplikace.mvcr.cz/sbirka/2007/sb041-07.pdf>.

[50] Zákon č. 124/2008 ze dne 19.března 2008 kterým se mění zákon číslo 269/1994 Sb., o Rejstříku trestů, ve znění pozdějších předpisů, a některé další zákony. In *Sbírka zákonů České republiky*. 2008, částka 39, s. 1544-1567. Dostupný také z WWW: <http://aplikace.mvcr.cz/archiv2008/sbirka/2008/sb039-08.pdf>.

# Seznam obrázků

# Seznam tabulek

# Seznam grafů

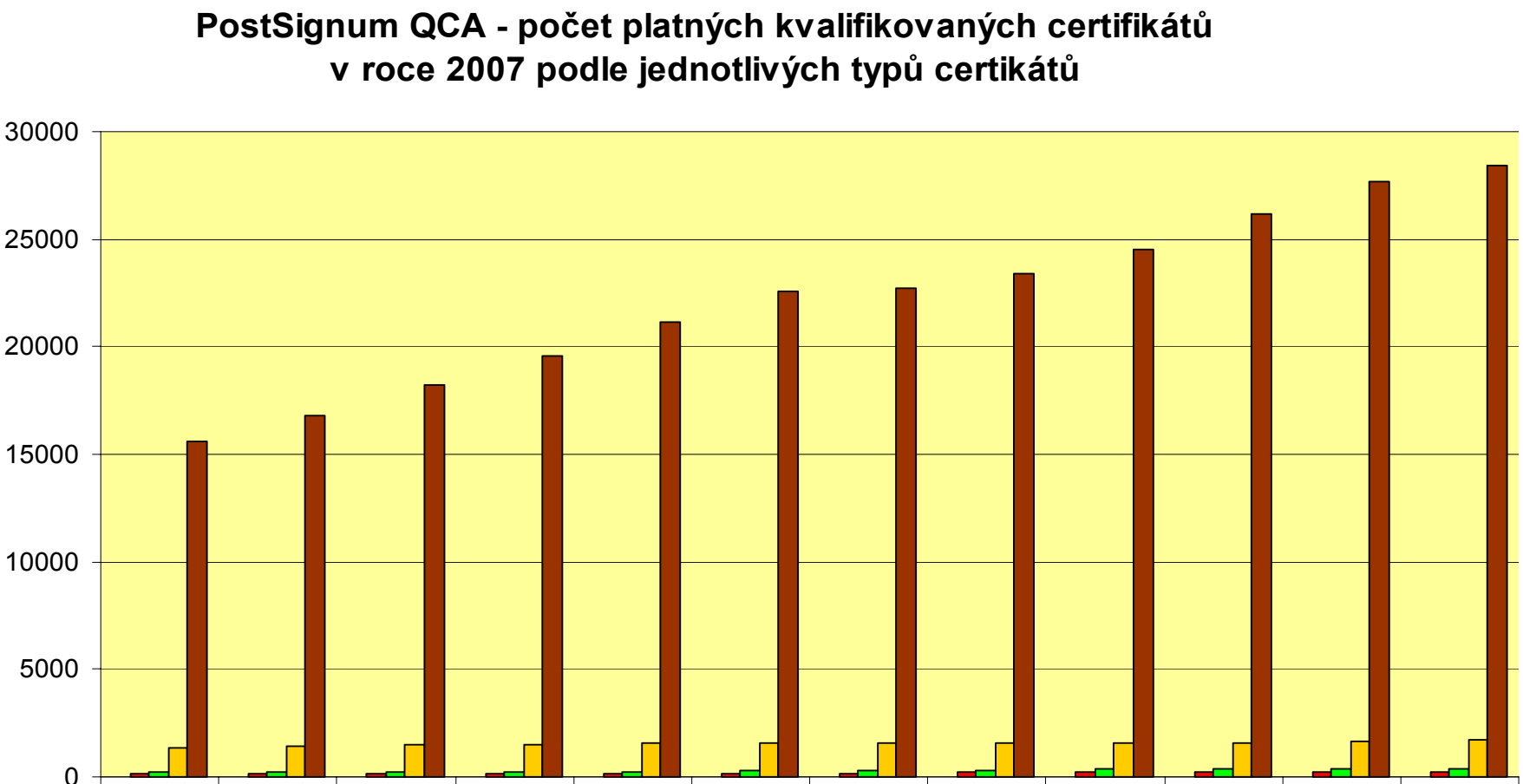
# Seznam zkratek

| | |
|---|---|
| ASN.1 | Abstract Syntax Notation, jazyk určený pro popis obecných datových struktur |
| BER | Basic Encoding Rules, kódování |
| CS HK | Celní správy Hradec Králové |
| CS PA | Celní správa Pardubice |
| Czech POINT | Český podávací ověřovací informační národní terminál |
| ČR | Česká republika |
| ČSSZ | Česká správa sociálního zabezpečení |
| DAP | Daňové přiznání |
| DES | Data Encryption Standard, šifrovací algoritmus |
| DPH | Daň z přidané hodnoty |
| DSS | Digital Signature Standard, šifrovací algoritmus |
| DV-certifikát | Data validation-certifikát, typ certifikátu časového razítka |
| EC | Eliptic Curve, šifrovací algoritmus |
| EP | Elektronický podpis |
| EU | Evropská unie |
| IDEA | International Data Encryption Algorithm, šifrovací algoritmus |
| MD5 | Message Digest 5, hashovaní algoritmus |
| MF ČR | Ministerstvo financí |
| MPSV | Ministerstvo práce a sociálních věcí |
| OSSZ PA | Okresní správa sociálního zabezpečení Pardubice |
| PKI | Public-Key Infrastructure, infrastruktura s veřejným klíčem |
| PVT | Podnik výpočetní techniky |
| RC2 | Rivest Cipher 2, šifrovací algoritmus |
| RC4 | Rivest Cipher 4, šifrovací algoritmus |
| RM | Registrační místo |

| | |
|---|---|
| RSA | Rivest Shamir Aleman, šifrovací algoritmus |
| RT | Rejstřík trestů |
| Sb. z. | Sbírky zákonů |
| SHA-1 | Secure Hash Algorithm, hashovaní algoritmus |
| SPD | Spotřební daň |
| USB | Universal Serial Bus, sériové rozhraní pro připojení periférií |

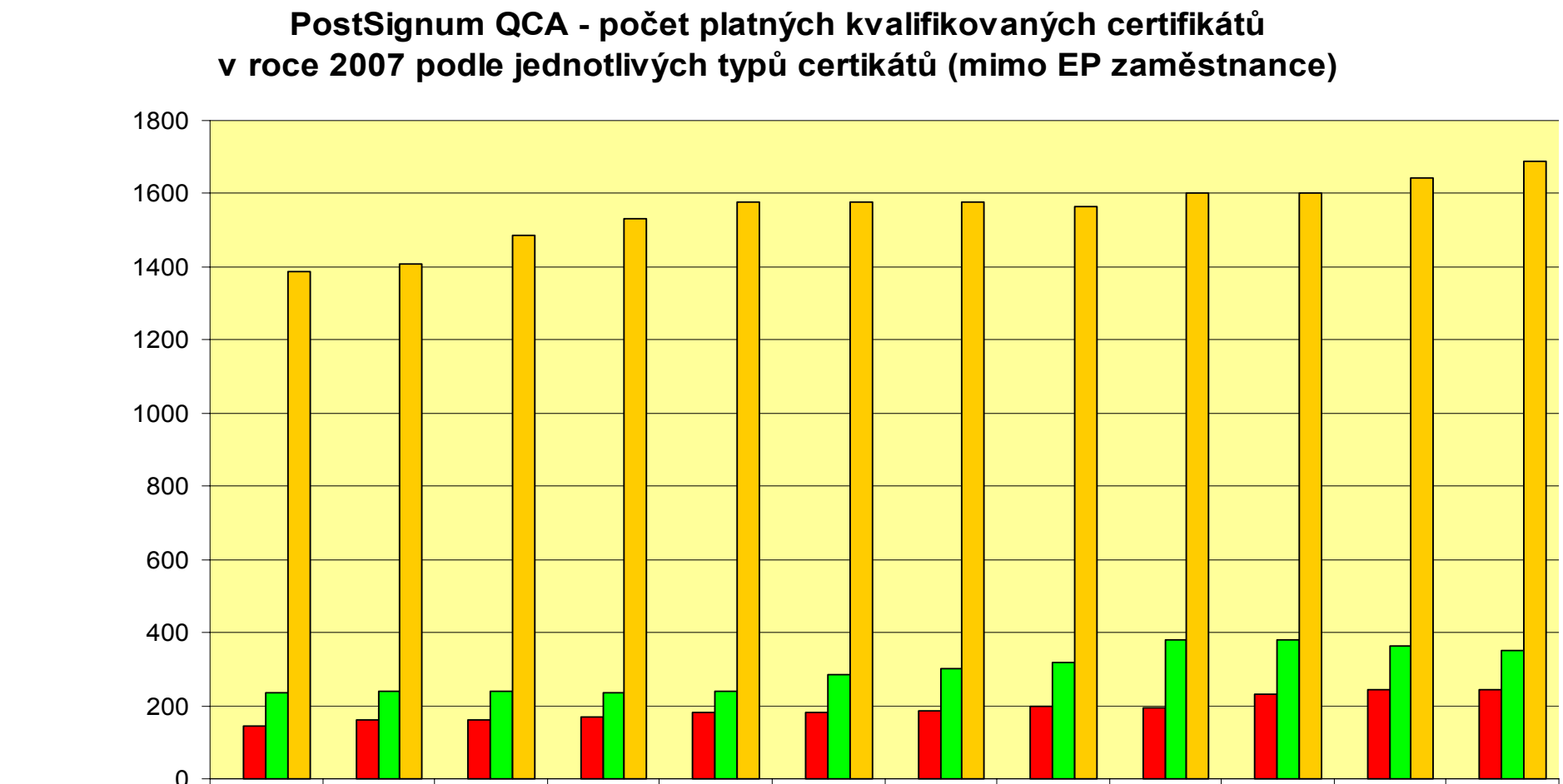
# Seznam příloh

**Příloha 1 PostSignum QCA - počet platných kvalifikovaných certifikátů v roce 2007 podle jednotlivých typů, zdroj vlastní – upraveno na základě [37]**



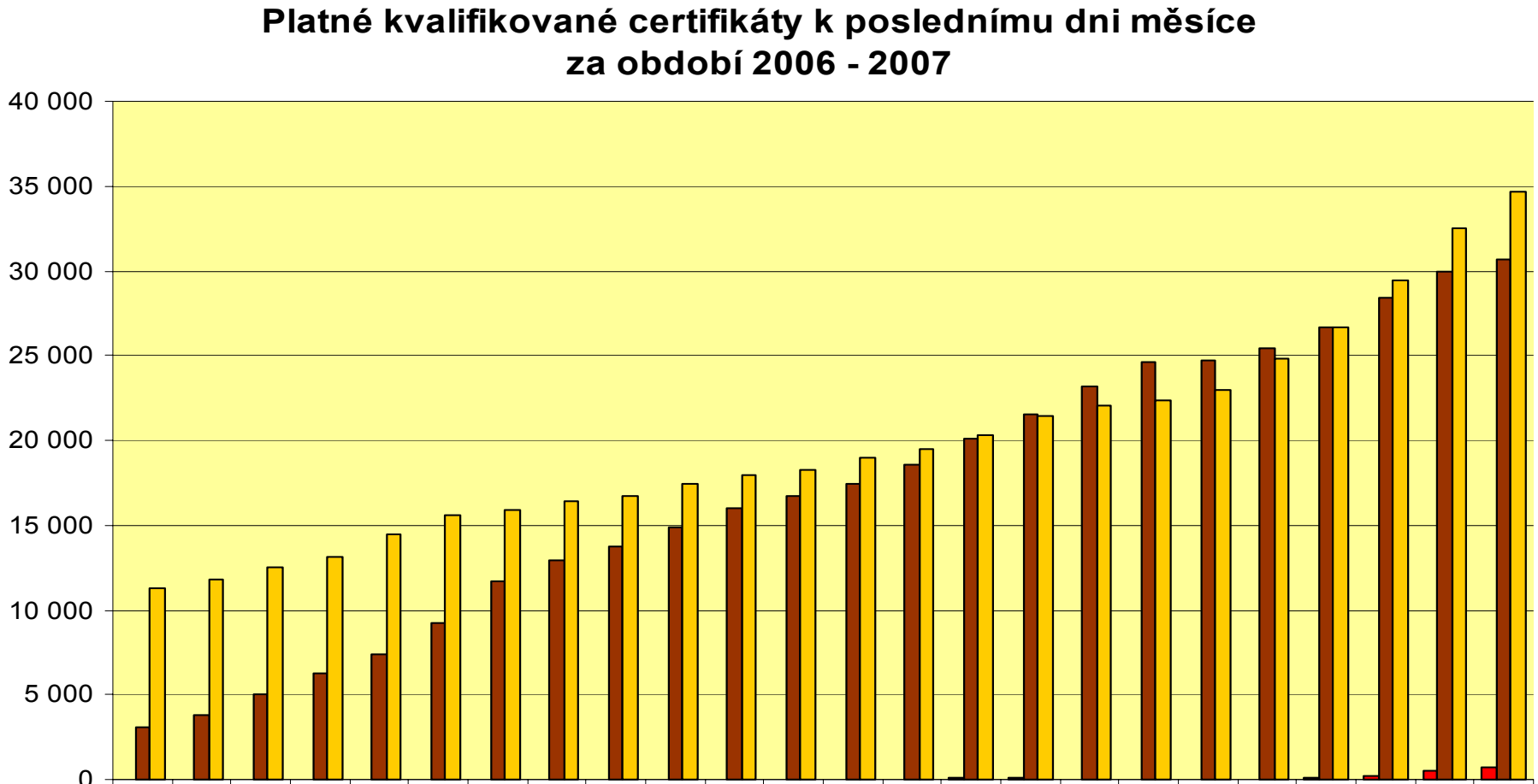

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| el. značka fyzické osoby | 2 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |
| el. značka organizace | 146 | 160 | 163 | 170 | 182 | 183 | 187 | 200 | 194 | 233 | 244 | 245 |
| "služební" certifikáty | 236 | 240 | 239 | 234 | 241 | 284 | 301 | 319 | 380 | 381 | 364 | 349 |
| el. podpis fyzické osoby | 1386 | 1409 | 1488 | 1532 | 1579 | 1578 | 1579 | 1564 | 1601 | 1603 | 1645 | 1689 |
| el. podpis zaměstnance | 15627 | 16769 | 18250 | 19578 | 21132 | 22595 | 22701 | 23396 | 24526 | 26144 | 27664 | 28414 |

**Příloha 2 PostSignum QCA - počet platných kvalifikovaných certifikátů v roce 2007 podle jednotlivých typů, zdroj vlastní – upraveno na základě [37]**




| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| el. značka fyzické osoby | 2 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |
| el. značka organizace | 146 | 160 | 163 | 170 | 182 | 183 | 187 | 200 | 194 | 233 | 244 | 245 |
| "služební" certifikáty | 236 | 240 | 239 | 234 | 241 | 284 | 301 | 319 | 380 | 381 | 364 | 349 |
| el. podpis fyzické osoby | 1386 | 1409 | 1488 | 1532 | 1579 | 1578 | 1579 | 1564 | 1601 | 1603 | 1645 | 1689 |

**Příloha 3 Vývoj počtu platných kvalifikovaných certifikátů za období 2006 a 2007, zdroj vlastní – upraveno na základě [10,24,26]**




| | I 2006 | II 2006 | III 2006 | IV 2006 | V 2006 | VI 2006 | VII 2006 | VIII 2006 | IX 2006 | X 2006 | XI 2006 | XII 2006 | I 2007 | II 2007 | III 2007 | IV 2007 | V 2007 | VI 2007 | VII 2006 | VIII 2007 | IX 2007 | X 2007 | XI 2007 | XII 2007 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| eIdentity | 16 | 13 | 9 | 8 | 8 | 8 | 9 | 9 | 6 | 4 | 10 | 14 | 17 | 19 | 52 | 65 | 34 | 39 | 48 | 47 | 103 | 156 | 483 | 754 |
| Česká pošta, s.p. | 3 048 | 3 836 | 5 013 | 6 210 | 7 338 | 9 235 | 11 642 | 12 937 | 13 707 | 14 886 | 15 959 | 16 728 | 17 397 | 18 580 | 20 141 | 21 515 | 23 135 | 24 641 | 24 769 | 25 480 | 26 702 | 28 361 | 29 917 | 30 697 |
| I.certifikační | 11 274 | 11 751 | 12 494 | 13 080 | 14 453 | 15 602 | 15 947 | 16 452 | 16 673 | 17 431 | 17 917 | 18 271 | 18 969 | 19 536 | 20 282 | 21 445 | 22 100 | 22 333 | 23 023 | 24 770 | 26 616 | 29 473 | 32 535 | 34 684 |

**Příloha 4 Žádosti o výpis nebo opis z Rejstříku trestů, zdroj vlastní – upraveno na základě [15]**


| | VII 2006 | VIII 2006 | IX 2006 | X 2006 | XI 2006 | XII 2006 | I 2007 | II 2007 | III 2007 | IV 2007 | V 2007 | VI 2007 | VII 2007 | VIII 2007 | IX 2007 | X 2007 | XI 2007 | XII 2007 | I 2008 | II 2008 | III 2008 | IV 2008 | V 2008 | VI 2008 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| počet vydaných | 196 | 4232 | 5935 | 7495 | 8330 | 7745 | 11634 | 10241 | 14363 | 13845 | 15957 | 17535 | 18072 | 25273 | 34881 | 47235 | 50110 | 37404 | 119672 | 133073 | 137130 | 140609 | 122906 | 129955 |