Elektronická komunikace s daňovou správou

Bc. Erika Ondroušková

Diplomová práce
2006

Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky

Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky
Ústav financí a účetnictví
akademický rok: 2005/2006

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Erika ONDROUŠKOVÁ**
Studijní program:	**N 6202 Hospodářská politika a správa**
Studijní obor:	**Finance**
Téma práce:	**Elektronická komunikace s daňovou správou**

Zásady pro vypracování:

Úvod

I. Teoretická část

- **Proveďte literární průzkum a na základě teoretických pramenů formulujte podstatu a význam elektronického podpisu.**
- **Analyzujte základní právní podmínky nutné pro vytváření a používání elektronického podpisu.**

II. Praktická část

- **Popište realizaci elektronického podpisu na pracovišti.**
- **Proveďte průzkum využití elektronického podání daňových přiznání.**
- **Na základě zjištěných výsledků vyhodnoťte současnou elektronickou komunikaci s daňovou správou.**

Závěr

Rozsah práce: **cca 70 stran**

Rozsah příloh:

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

Seznam odborné literatury:

1. BOSÁKOVÁ, D.,aj. Elektronický podpis.1.vyd.Olomouc: ANAG, 2002. ISBN 80-7263-125-X

2. DOBDA, L. Ochrana dat v informačních systémech. 1.vyd. Praha: Grada Publishing,1999, ISBN 80-7169-479-7

3. JAŠEK, R. Ochrana znalostí a dat v podnikových informačních systémech. 1. vyd.Zlín: UTB Zlín 2002. ISBN 80-7318-095-2

4. RYBKA, M. Jak komunikovat elektronicky. 1. vyd. Praha: Grada Publishing, 2002.ISBN 80-247-0208-8

5. http://www.mfcr.cz

Vedoucí diplomové práce: **Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a statistiky

Datum zadání diplomové práce: **6. března 2006**

Termín odevzdání diplomové práce: **12. května 2006**

Ve Zlíně dne 6. března 2006

L.S.

doc. PhDr. Vnislav Nováček, CSc.
děkan

doc. Dr. Ing. Drahomíra Pavelková
ředitel ústavu

ABSTRAKT

Diplomová práce Elektronická komunikace s daňovou správou si klade za cíl analýzu stávající situace elektronického podpisu v oblasti práva s návazností na jeho praktickém využití v daňové správě. Vzhledem k aktuálnosti a obecné neznalosti daného problému, vychází řadě médií články, které tuto problematiku značně zkreslují a zamlžují. V této práci se tedy pokusím objektivně popsat problematiku elektronického podpisu, provést průzkum využití elektronického podání daňových přiznání a na základě zjištěných výsledků vyhodnotit současnou elektronickou komunikaci s daňovou správou.

Klíčová slova: elektronický podpis, kvalifikovaný certifikát, autority, elektronické podatelny, elektronické daňové řízení, elektronické podání daňových přiznání.

ABSTRACT

The goal of the diploma paper The electronic communication with the tax office is to analyse the present situation of the digital signature in the sphere of law as well as the practical usage of the digital signature in the tax administration. A great number of confusing articles about this subject have been published in regard to the topicality and general ignorance of the problem. The aim of the diploma paper is to describe objectively the questions of the digital signature and carry out the survey of the usage of the electronic tax return submission. The current situation of the electronic communication with the tax office will be analysed on the basis of the results of the aforesaid investigation.Abstrakt ve světovém jazyce

Keywords: digital signature, qualified certificate, authorities, electronic registry, elektronic tax procedure, elektronic tax return submission

Čestné prohlášení

Prohlašuji, že jsem diplomovou práci zpracovala samostatně a použitou literaturu jsem citovala.

Ve Zlíně 12. 5. 2006 ……..

OBSAH

ÚVOD

V dnešní době již neexistuje oblast našeho života, kde bychom se nesetkali s počítačem. V zaměstnání, v obchodě, u lékaře, samozřejmě v bance, ale zcela určitě na kterémkoli úřadě veřejné či státní správy přicházíme do styku s výpočetní a informační technikou. Postupný přechod od papírových dokumentů k elektronickým probíhá všude ve světě a všude ve světě je tedy problém zrovnoprávnění elektronického zápisu s papírovým z hlediska zákona více než aktuální. Některé právní řády umožňují výkladem svých norem nelpět na konkrétním nosiči informací, ale speciálně v podmínkách kontinentálního právního systému, je třeba technologické možnosti podložit právní úpravou.

Klíčovou roli v této problematice hraje právě podpis, resp. elektronický podpis. E-podpis se dá využít všude tam, kde je dnes nutné úřední razítko či ruční podpis občana nebo úředníka. Všechny dokumenty, které zatím známe v papírové podobě, lze převést na dokumenty elektronické a všechny podpisy je možné nahradit jejich elektronickou formou. Podepisovat i ověřovat podpisy lze takto nesrovnatelně rychleji a efektivněji. Je možné podepsat dokonce i to, co lze ručně opatřit podpisem jen velmi těžko – obsah diskety, fotografii, přístupy do databáze apod.

Zakotvení elektronického podpisu a očekávaný následný rozvoj elektronické komunikace může vnést zcela nové směry do výkonu veřejné i státní správy, kdy lze reálně očekávat vytvoření možnosti styku občana a úřadu prostřednictvím elektronické pošty (z domu, zaměstnání či tzv. internetových kiosků). Tímto způsobem si tedy lze představit zasílání daňových přiznání, odhlášení motorového vozidla nebo jiných úředních dokumentů.

.

I. TEORETICKÁ ČÁST

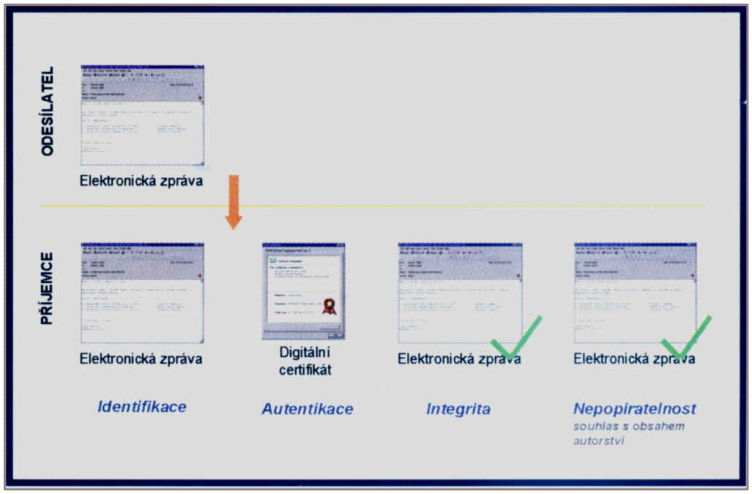
1 VÝZNAM A PODSTATA ELEKTRONICKÉHO PODPISU

Elektronický podpis je v dnešní době nová, postupně se zavádějící technologie, jejímž cílem je vedle klasického podpisu postavit nástroj, který dostatečně potvrzuje autorství dotyčného člověka. Má tedy být v kybernetickém světě tím, čím je běžný podpis v normální životě. Není to ovšem tak jednoduché, jak se na první pohled může zdát. Název totiž do jisté míry vede k vytváření některých předsudků a nepochopení, které mají základ v rozdílnosti obou světů [Jašek 3].

Elektronická pošta pro řadu lidí zajišťuje velmi významnou část z celkového objemu denní komunikace. Zvykli jsme si elektronické poště důvěřovat, ale můžeme si být stoprocentně jisti odesílatelem? Určitě ne. Technicky je velmi snadné přepsat hlavičku e-mailu tak, aby adresát nepoznal, kdo je skutečným autorem zprávy. Přepíšeme v hlavičce jméno a e-mailovou adresu odesílatele a sdělené informace jsou podvrženy – jak snadné. Nasazením elektronického podpisu však máme k dispozici spolehlivé a velmi efektivní řešení [5].

1.1 Přínos u příjemce elektronicky podepsané zprávy

Identifikaci – z přijaté zprávy musí jednoznačně vyplývat, od koho pochází, tedy kdo je jejím autorem. Údaj o autorovi musí být dostatečně věrohodný, pouhá hlavička e-mailu nestačí. Autora určuje *identifikace*, ověření skutečné identity se nazývá *autentikace.* (V tomto případě obě tyto vlastnosti hodně splývají). Příjemce chce mít kromě toho jistotu i o obsahu zprávy. Byla zpráva od svého podepsání změněna? Jedná se o vlastnost nazvanou *integrita*, která zaručuje neporušenost obsahu zprávy. Další významnou vlastností je *nepopiratelnost*. Autor nemůže později popřít autorství zprávy, resp. souhlas s obsahem zprávy. Jedná se tedy o téměř dokonalou analogii s podpisem vlastnoručním. Pokud tedy příjemce obdrží od někoho elektronickou zprávu opatřenou elektronickým podpisem, může si být jistý jednak autorem zprávy, dále tím, že zpráva nebyla od svého elektronického podepsání pozměněna. Má také jistotu, že autor nemůže v budoucnu popřít autorství příslušné zprávy [5]. V kombinaci se šifrováním je možné docílit efektu, díky němuž je možné provést ověření podpisu až po úspěšném rozšifrování zprávy. Zpráva je tedy chráněna před vyzrazením jejího obsahu. Toto je jistě výrazně dokonalejší podoba zalepené poštovní obálky [Jašek 3].



Obr. 1. Vlastnosti elektronicky podepsané zprávy. Převzato z [11].

1.2 Elektronické podepisování zpráv

Vlastní podepsání elektronického dokumentu je celkem jednoduché, a to hlavně z toho důvodu, že za celý průběh zodpovídá specializovaný software, takže uživatel pouze zvolí dokument a vydá potřebný příkaz.

Základním předpokladem pro to, abychom mohli svůj elektronický podpis připojit k dokumentům, jejichž platnost chceme jeho prostřednictvím stvrdit, je přidělení dvou „klíčů“ – privátního a veřejného, a certifikátu. Získat je může každý zájemce u poskytovatele, jehož zákon nazývá certifikační autoritou (tím je jasně řečeno i to, že tato právnická osoba garantuje, proto je i autoritou, že klíč skutečně vydala a je tudíž platný).

Privátní klíč slouží samotnému uživateli, který jeho prostřednictvím příslušný dokument „podepíše“ a tím jej jednoznačně identifikuje. Privátní klíč je určen výhradně pro uživatele, jemuž byl vydán a je samozřejmě zabezpečen běžnými prostředky, jako je heslo. Ostatně vzhledem k tomu, že podpis prostřednictvím privátního klíče je právně uznávanou formou stvrzení platnosti,může mít zneužití pro uživatele velmi nepříjemné důsledky, a je proto v zájmu všech se o svůj privátní klíč starat.

Veřejný klíč, jak už název naznačuje, je naopak určen široké veřejnosti a slouží k ověřování platnosti elektronického podpisu, resp. důvěryhodnosti dokumentu elektronickým podpisem signovaného.

Certifikát je datová zpráva, která předává data nutná k ověření elektronického podpisu. Vystavují je právě certifikační autority, tedy důvěryhodné organizace k poskytování těchto služeb oprávněné. Certifikát přitom musí obsahovat celou řadu položek, které dle novely zákona č. 227/2000 Sb., o elektronickém podpisu , přesně identifikují osobu, která certifikát využívá [5].

K pochopení, jak vlastní podepsání dokumentu funguje je potřeba dále znát ještě dva pojmy - hash a asymetrickou šifru.

Hash, neboli otisk dokumentu se vytváří prostřednictvím hashovací funkce, jež z libovolně dlouhé zprávy (dokumentu) vytvoří její otisk. Pokud se ve zprávě následně změní jediné písmeno, otisk se bude lišit. Z otisku přitom nejde určit původní text a v rozumném čase ani najít text, který by měl otisk shodný s původním textem [10].

Elektronické podepisování zprávy probíhá tak, že se pomocí jednocestné funkce (hash funkce) vytvoří tzv. otisk zprávy, který je zašifrován soukromým klíčem a přidán k této zprávě. Příjemce dešifruje získaný zašifrovaný otisk veřejným klíčem (obsaženým v certifikátu) a zpět za pozici hash funkce vygeneruje ze zprávy nebo datového souboru nový otisk, přičemž oba porovná. Pokud jsou totožné, je zřejmé, že nedošlo k žádným úpravám zasílaných informací a odesílatel byl identifikován a ověřen [Jašek 3].

Asymetrická šifra je postavena na již zmíněných dvou klíčích - privátním a veřejném, přičemž, jak již bylo řečeno, jeden slouží k šifrování a druhý k dešifrování.

1.3 Ověřování pravosti podpisu

Ověřování pravosti podpisu se děje obdobným způsobem. Elektronický podpis je příslušným počítačovým programem ověřen v případě, že kontrolní výpočty souhlasí při jejich porovnání s původními hodnotami. Pokud k této kontrole nedojde, znamená to, že data byla modifikována (mohla být změněna i odesílatelem zprávy). Elektronický podpis pozbývá v tomto případě platnosti [Jašek 3].

1.4 Digitální podpis

V souvislosti s elektronickou autentizací se vedle termínu „elektronický podpis“ objevuje i termín „digitální podpis“. Zákonitě vyvstává otázka rozdílu mezi těmito označeními. Elektronický podpis je širším termínem, který zahrnuje vedle výše uvedeného také například biometrické prokazování totožnosti (otisk prstu, snímání oční rohovky..) nebo jiné prokázání totožnosti (například čipová karta, nebo něco co dotyčná osoba jednoznačně vlastní). Digitální podpis je speciálním případem elektronického podpisu, kdy k ověření původu dokumentu dochází na základě šifrování [Jašek 3].

2 PŘEHLED PLATNÉ PRÁVNÍ ÚPRAVY V ČR

Česká republika se zařadila mezi první evropské země, které legalizovaly moderní elektronickou formu zpracování dokumentů. Stalo se tak 1. října 2000, kdy nabyl účinnosti zákon č. 227/2000 Sb., o elektronickém podpisu. Význam a důsledky tohoto zákona přesahují běžné legislativní úpravy. Schválením tohoto zákona byla uskutečněna novela všech hlavních procesních norem: občanského soudního řádu, správní řádu, trestního řádu a zákona o správě daní a poplatků, v nichž byla zakotvena alternativní možnost elektronického podání opatřeného zaručeným elektronickým podpisem. Rovněž byla provedena novela § 40 občanského zákoníku upravujícího podepisování [12]. Zákon o elektronickém podpisu a o změně některých dalších zákonů je zcela samozřejmě zaměřen na právní aspekty problematiky mnohem více než na technické řešení. Vzhledem k překotnému vývoji v technologii podpisových schémat by tak měl zůstat zákon pevným bodem pro výchozí technické aplikace elektronického podpisu. Ty jsou naopak předmětem prováděcí Vyhlášky Úřadu pro ochranu osobních údajů [13]. Prováděcí vyhláška má za úkol doplňovat zákon o elektronickém podpisu konkrétními požadavky kladenými jak na uživatele e-podpisu, tak na tzv. důvěryhodné strany.

Tyto dva akty spolu tvoří stavební kámen rozvoje elektronického podpisu, potažmo rozvoje elektronického obchodu v České republice, komunikace s veřejnou a daňovou správou.

2.1 Zákon č. 227/2000 o elektronickém podpisu

2.1.1 Vznik zákona o elektronickém podpisu

Zákon vznikl na základě iniciativy podnikatelské sféry (konkrétné Sdružení pro informační společnosti nebo SPIS) a poslanců Parlamentu ČR. Jeho autorem je skupina odborníků v oblasti IT a práva vedená doc. Smejkalem a doc. Matesem. Zákon o elektronickém podpisu byl poskytnut k diskusi celé odborné veřejnosti a po zapracování značného množství připomínek byl předložen vládě 8. 11. 1999 jako poslanecká iniciativa místopředsedů čtyř politických stran: I. Langera, S. Grosse, V. Mlynáře a C. Svobody. Vláda tento návrh odmítla a vrátila jej k přepracování tak, aby zákon odpovídal požadavkům směrnice EU 1999/93/EC [14]. V květnu 2000 schválila Poslanecká sněmovna parlamentu téměř jednohlasně poslanecký návrh zákona o elektronickém podpisu a změně některých dalších záko-

nů. Posléze s ním vyslovil souhlas senát a 10. července jej podepsal i prezident republiky. Dne 1. října 2000 vstoupil v platnost.

2.2 Proč potřebujeme elektronický podpis

- Je téměř nemožné jej zfalšovat.
- Je velice jednoduché ověřit pravost tohoto podpisu a dojít tak k jednoznačnému a správnému rozhodnutí, zda je podpis platný, či nikoliv. U klasického podpisu je nutný podpisový vzor a je vysoce reálná možnost přehlédnutí některých detailních rozdílů porovnávaných podpisů.
- Vždy je zaručena neporušenost zprávy a my můžeme prohlásit, že obsah zprávy je stejný s obsahem v době podpisu.Tomuto říkáme ověřování integrity zprávy.

O elektronickém podpisu můžeme také prohlásit, že má vlastnost nepopiratelnosti. V praxi to znamená, že podepsaná osoba nemůže podepsat prázdný papír, jehož obsah bude doplněn později. Díky této vlastnosti podepsaná osoba nemůže popřít, že nebyla seznámena s obsahem dané zprávy a že ji tudíž neodeslala ona [Bosáková 1].

2.3 Vymezení některých pojmů

Pro účely tohoto zákona se rozumí elektronickým podpisem údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě, zaručeným elektronickým podpisem, elektronický podpis, který splňuje následující požadavky:

- Je jednoznačně spojen s podepisující osobou.
- Umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě.
- Byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou.
- Je k datové zprávě, ke které se vztahuj, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat, [12].

V § 3 odst. 2 zákona o elektronickém podpisu se dále o zaručeném elektronickém podpisu říká, že použití zaručeného elektronického podpisu založeného na kvalifikovaném certifi-

kátu a vytvořeného pomocí prostředku pro bezpečné vytváření podpisu umožňuje ověřit, že datovou zprávu podepsala osoba uvedená na tomto kvalifikovaném certifikátu [12]. Zaručený elektronický podpis podle § 4 , který zní: použití zaručeného elektronického podpisu zaručuje, že dojde-li k porušení obsahu datové zprávy od okamžiku, kdy byla podepsána, toto porušení bude možno zjistit, umožňuje ověření souladu přijaté datové zprávy s podepsanou datovou zprávou nebo-li originálem [12].

V dalším textu zákona není nijak upraveno používání ani další vlastnosti „běžného“ elektronického podpisu. Praktické použití elektronického podpisu není tedy podloženo zákonem a je tedy nutné vztahy, založené na tomto elektronickém podpisu, upravit smluvně podle principu smluvní volnosti [12]. V případě, že by neexistovala smluvní úprava vztahů zúčastněných stran, která by řešila spor založený na běžném elektronickém podpisu, mohl by být za určitých okolností v rámci důkazního řízení vyhodnocen elektronický popis jako zaručený elektronický podpis a spor by se řešil podle zákona o elektronickém podpisu. ZoEP podporuje běžný elektronický podpis jen minimálně.

Zaručený elektronický podpis, který splňuje požadavky § 2 písm. b) ZoEP, byl vytvořen pomocí prostředků pro bezpečné vytváření elektronického podpisu (§ 2 písm. m) a je založený na kvalifikovaném certifikátu (§ 2 písm. h) již dává oběma stranám záruky dle zákona [12].

2.4 Prostředek pro bezpečné vytváření elektronického podpisu

Zákon dále rozlišuje pojmy prostředek pro vytváření elektronických podpisů a prostředek pro bezpečené vytváření elektronických podpisů. § 2 písm. k) ZoEP zní: prostředkem pro vytváření elektronických podpisů se rozumí technické zařízení nebo programové vybavení, které se používá k vytváření elektronických podpisů [12]. Prostředek pro bezpečné vytváření elektronických podpisů je definován v § 2 písm. m) takto: prostředkem pro bezpečné vytváření elektronických podpisů se rozumí prostředek pro vytváření elektronického podpisu, který splňuje požadavky stanovené tímto zákonem [12]. Akreditovaní poskytovatelé a poskytovatele certifikačních služeb vydávající kvalifikované certifikáty jsou podle § 3 odst. 2) a § 6 písm. j) povinni používat bezpečné systémy a nástroje elektronického podpisu, jejichž součástí jsou prostředky pro bezpečné vytváření elektronických podpisů. Prostředky pro ověřování elektronického podpisu a prostředky pro bezpečné ověřování elektronického podpisu jsou též zákonem analogicky rozlišeny. ZoEP v § 17 stanovuje požadavky na tyto bezpečné prostředky. Používání běžných prostředků pro vytváření a ověřo-

vání elektronického podpisu zákon nijak neupravuje. Zákon poskytuje oporu pro elektronický podpis takový, jaký je definován v § 3 odst. 2), čili podpis vytvořený zmíněnými prostředky pro bezpečné vytváření elektronického podpisu.

2.5 Kvalifikovaný certifikát

V ZoEP se dále rozlišují pojmy certifikát a kvalifikovaný certifikát. Podle § 2 písm. g) ZoEP se certifikátem rozumí datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování podpisů s podepisující osobou a umožňuje ověřit její totožnost [12]. Certifikát tedy nemusí obsahovat informace o totožnosti osoby, musí ale obsahovat data identifikující podepisující osobu. Musí zde být též možnost, pomocí těchto dat, zjistit totožnost podepisující osoby. Totožnost osoby prokáže poskytovatel certifikačních služeb. Zákon neklade na běžný certifikát žádná další omezení. Běžný certifikát má tedy vůči kvalifikovanému certifikátu podobnou váhu jako elektronický podpis a zaručený elektronický podpis [10]. V § 6 odst. 7) ZoEP však stojí, že poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty, musí neprodleně ukončit platnost certifikátu, pokud o to podepisující osoba požádá nebo v případě, že byl certifikát vydán na základě nepravdivých nebo chybných údajů [12].

Kvalifikovaný certifikát je takový certifikát, který splňuje požadavky § 2 písm. h): certifikát, který má náležitosti stanovené tímto zákonem a byl vydán poskytovatelem certifikačních služeb, splňujícím podmínky, stanovené tímto zákonem pro poskytovatele certifikačních služeb vydávající kvalifikované certifikáty [12]. Zákon stanoví náležitosti kvalifikovaného certifikátu v § 12. Abychom mohli označit certifikát za kvalifikovaný, musí být vydán poskytovatelem certifikačních služeb vydávající kvalifikované certifikáty, který splňuje podmínky § 6 ZoEP.

2.6 Poskytovatelé certifikačních služeb

Zákon dále definuje a rozlišuje tři úrovně poskytování certifikačních služeb. Poskytovatelem certifikačních služeb je subjekt – instituce, certifikační autorita, který vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy [12]. Tři kategorie certifikačních autorit:

- Poskytovatel certifikačních služeb.
- Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty.
- Akreditovaný poskytovatel certifikačních služeb.

Přestože v praxi nemusí být ve způsobu jejich fungování a tudíž ve spolehlivosti a důvěryhodnosti jejich služeb žádný rozdíl, je třeba upozornit na jejich právní uznatelnost vycházející z jejich postavení. „Obyčejná“ certifikační autorita například nemusí splňovat žádné legislativní požadavky a její činnost není nikým kontrolována. Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty a Akreditovaný poskytovatel certifikačních služeb musí splňovat přísná ustanovení Zákona bezpečnosti jejich provozu, náležitostí kvalifikovaného certifikátu apod. Nad dodržováním veškerých legislativních požadavků vykonává dozor Úřad pro ochranu osobních údajů s pravomocí rozsáhlých sankcí v případě jejich porušení.

Na mnohem vyšší úrovni je v zákoně definován institut poskytovatele certifikačních služeb vydávající kvalifikované certifikáty. Povinnosti poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty jsou předmětem § 6 ZoEP. § 6 mimo jiné ukládá poskytovateli:

- Zajistit, aby kvalifikované certifikáty jím vydané odpovídaly ZoEP.
- Bezpečně ověřit totožnost osoby.
- Zjistit, zda data pro vytváření elektronických podpisů odpovídají datumům pro ověřování elektronických podpisů, která obsahuje kvalifikovaný certifikát.
- Vedení a zpřístupnění seznamu platných a zneplatněných certifikátů.
- Používat bezpečné nástroje elektronického podpisu schválené Úřadem pro ochranu osobních údajů.
- Uchovávat veškeré informace a dokumentaci o vydaných kvalifikovaných certifikátech po dobu nejméně 10 let od data zneplatnění.
- Vést provozní dokumentaci o veškeré činnost poskytovatele i s vydanými kvalifikovanými certifikáty.

Kvalifikované certifikáty vydává poskytovatel certifikačních služeb podepisujícím osobám na základě smlouvy. Smlouva musí být písemná, jinak je neplatná [12]

Na nejvyšší úrovni stojí instituce akreditovaného poskytovatele certifikačních služeb.

Dle § 10 odst. 1) může každý poskytovatel certifikačních služeb požádat Úřad o udělení akreditace pro výkon činnosti akreditovaného poskytovatele certifikačních služeb. Působnost této normy je omezen § 10 odst. 7): součástí rozhodnutí Úřadu o akreditaci je ověření kvalifikovaného certifikátu poskytovatele certifikačních služeb Úřadem [12]. Poskytovatel tedy musí vydávat kvalifikované certifikáty. V § 10 odst. 5) a 6) se dále zužuje okruh možných kandidátů na akreditovaného poskytovatele. Tím může být pouze poskytovatel se sídlem na území České republiky a zároveň, kromě činností uvedených v ZoEP, může akreditovaný poskytovatel certifikačních služeb bez souhlasu Úřadu působit jen jako advokát, notář nebo znalec [12]. Obsah žádosti o akreditaci je stanoven v § 10 odst. 2). Výhodou akreditace je možnost působení v oblasti orgánů veřejné moci (§ 11). Toto působení se týká komunikace mezi samotnými orgány veřejné moci a též mezi veřejností a jednotlivými orgány veřejné moci. Podle § 9 odst. 2) ZoEP, vykonává Úřad nad akreditovanými poskytovateli dozor, uděluje a odnímá akreditace, ukládá jim opatření k nápravě a pokuty za porušení povinností podle tohoto zákona, vede a uveřejňuje seznam akreditovaných poskytovatelů, vyhodnocuje shodu nástrojů elektronického podpisu s požadavky stanovenými tímto zákonem a prováděcí vyhláškou a plní další povinnosti stanovené ZoEP. Za účelem výkonu dozoru je akreditovaný poskytovatel certifikačních služeb vydávající kvalifikované certifikáty povinen pověřeným zaměstnancům Úřadu umožnit v nezbytně nutném rozsahu vstup do obchodních a provozních prostor, na požádání předložit veškerou dokumentaci, záznamy, doklady, písemnosti a jiné podklady související s jeho činností, umožnit jim v nezbytně nutné míře přístup do svého informačního systému a poskytnout informace a veškerou potřebnou součinnost - § 9 odst. 9) ZoEP. Tento odstavec se vztahuje pouze na akreditované poskytovatele certifikačních služeb. Je tedy otázkou, jakým způsobem bude Úřad provádět kontrolu certifikačních služeb vydávající kvalifikované certifikáty.

Pokud akreditovaný poskytovatel hodlá ukončit svou činnost, postupuje podle § 13 ZoEP. Zákon mu v takovém případě klade povinnost vynaložit veškeré možné úsilí na to, aby platné kvalifikované certifikáty byly převzaty jiným akreditovaným poskytovatelem certifikačních služeb. Není-li akreditovaný poskytovatel schopen zajistit, aby platné kvalifikované certifikáty převzal jiný akreditovaný poskytovatel certifikačních služeb, Úřad převezme evidenci vydaných kvalifikovaných certifikátů a oznámí to dotčeným podepisujícím osobám [12].

Jak bylo uvedeno, Úřad vykonává nad akreditovanými poskytovateli a poskytovateli certifikačních služeb vydávající kvalifikované certifikáty dozor. Zjistí-li, že akreditovaný po-

skytovatel certifikačních služeb nebo poskytovatel certifikačních služeb vydávající kvalifikované certifikáty porušuje povinnosti stanovené tímto zákonem, uloží mu, aby ve stanovené lhůtě sjednal nápravu, a případně určí, jaká opatření k odstranění nedostatku je tento poskytovatel certifikačních služeb povinen přijmou - § 14 odst. 1) ZoEP. V případě závažnějšího porušení zákona je Úřad oprávněn udělenou akreditaci odejmout a může současně ukončit platnost kvalifikovaných certifikátů vydaných dotyčným poskytovatelem.

2.7 Povinnosti podepisující osoby

Zákon působí též na podepisující osoby. Podepisující osoba je tedy podle § 5 odst. 1) povinna:

- Zacházet s prostředky, jakož i s daty pro vytváření zaručeného elektronického podpisu, s náležitou péči nepotřebné odborné úrovni tak, aby nemohlo dojít k jejich neoprávněnému použití [12].
- Uvědomit neprodleně poskytovatele certifikačních služeb, který jí vydal kvalifikovaný certifikát, o tom, že hrozí nebezpečí zneužití jejích dat pro vytváření zaručeného elektronického podpisu [12]. Zde je vyjádřena oznamovací povinnost ve vztahu k poskytovateli certifikačních služeb ohledně existence, byť sebemenší možnosti hrozby nebezpečí, zneužití programového vybavení, jehož je k podpisu užito.
- Podávat přesné, pravdivé a úplné informace poskytovateli certifikačních služeb ve vztahu ke kvalifikovanému certifikátu [12].

2.8 Povinnosti poskytovatele

Zákon o elektronickém podpisu stanoví odpovědnost poskytovatele certifikačních služeb. Tato je stanovena v § 7 odst. 1): za škodu způsobenou porušením povinností stanovených tímto zákonem odpovídá poskytovatel certifikačních služeb vydávající kvalifikované certifikáty podle zvláštních právních předpisů [12] (též Občanského zákoníku).

3 VYHLÁŠKA ÚŘADU PRO OCHRANU OSOBNÍCH ÚDAJŮ

Zákon o elektronickém podpisu tvoří teoretický a dosti obecný rámec pro používání elektronického podpisu. Svou technickou nezatížeností si klade nároky být jakýmsi stálým bodem na poli dynamicky se měnících informačních technologií. V souladu se směrnicí Evropské unie, na jejíchž základech vznikl, zůstává relativně abstraktní v definování práv a povinností zúčastněných stran při používání elektronického podpisu. Z těchto důvodů není možné, bez zavedení dalších právních předpisů, plně využívat možnosti, které samotný zákon poskytuje. Zákon totiž předpokládá existenci prováděcích vyhlášek, které jednak upraví konkrétní postupy používání elektronického podpisu v oblasti orgánů veřejné moci a které stanoví konkrétní požadavky na nástroje a subjekty podle § 6 a § 17 ZoEP.

Vyhláška má za úkol stanovit konkrétní technické parametry nástrojů a postupů při realizaci norem ZoEP. Aby bylo možné realizovat elektronický podpis a certifikace na nadnárodní úrovni, je nutné, aby systémy ostatních států používaly kompatibilní technologie. V tomto ohledu hledá a přejímá EU řadu technických norem pro elektronický podpis, které tento požadavek splňují. Na členských státech pak je, aby tyto normy začlenily do svých právních systémů. Proces specifikace a začleňování těchto norem do legislativy je vhledem k jejich důležitosti a složitosti velice náročná procedura a jako taková vyžaduje poměrně dost času [13].

3.1 Infrastruktura poskytování certifikačních služeb

Klíčovým mechanismem implementace soudobých IT aplikací provozovaných v otevřených sdílených sítích a požadujících záruky za autentičnost a bezpečnost, tedy i aplikací založených na používaní elektronických podpisů, je a zřejmě dlouho bude asymetrická kryptografie. Používání asymetrické kryptografie si vynucuje dostupnost pomocné infrastruktury pro důvěryhodné zveřejňování veřejných klíčů a identity jejich vlastníků a pro správu související s takovou činností.

3.2 Distribuce klíčů

Šifrování a podepisování informací vedle svých výhod vyžaduje i dodržování určitých pravidel. Ani sebelepší šifrovací mechanismus totiž nepřinese požadovaný bezpečnostní efekt, nemá-li důvěryhodnou distribuci, uložení a ničená svých šifrovacích a dešifrovacích klíčů. Zajistit jejich bezpečně uložení a ničení není zpravidla velký problém a lze jej reálně řešit. Velkým problémem je ovšem distribuce. Tato je řešena dvěma základními způsoby:

- Distribuce zajištěná certifikační autoritou.
- Distribuce zajištěná vzájemnou výměnou klíčů mezi uživateli. Toto řešení je ale vzhledem k užší vazbě na lidský faktor nejvíce rizikové.

3.3 Autority

Certifikační autority patří mezi entity bezpečnostních struktur, které souhrnně označujeme jako poskytovatele důvěryhodných služeb. Tyto podporují ustanovení vztahu důvěry mezi zúčastněnými stranami poskytováním podpůrných služeb – vydávají certifikáty, podporují křížové uznávání certifikátů vydávaných různými poskytovateli certifikačních služeb, generují časová razítka, udržují a vydávají seznamy neplatných certifikátů, umožňují on-line přístup do databáze certifikátů, přijímají požadavky na zneplatnění.

3.3.1 Certifikační autorita

Distribuce veřejných klíčů je optimálně řešena prostřednictvím důvěryhodné třetí strany, označované jako certifikační autorita. Tuto autoritu lze přirovnat ke státnímu notáři. Pod pojmem certifikát je možné si představit jistý průkaz totožnosti platný pro celý elektronický svět. Je to doklad o tom, že totožnost držitele veřejného klíče byla ověřena.

Certifikační autorita je institucí, jejímž úkolem je ověřovat a stvrzovat identitu držitelů veřejných klíčů a následně vydávat, evidovat a zveřejňovat, případně zneplatňovat již vydané certifikáty.

V souvislosti s certifikačními autoritami se objevuje pojem „registrační autority“. Jedná se o důvěryhodné subjekty, které jsou zřizovány pro provádění činností potřebných pro činnost certifikační autority. Úkolem registrační autority je autorizovaný sběr a ověřování informací o identitě žadatelů a certifikát a k určování informací, které je možné certifikační autoritou vložit do vytvářených certifikátů. Registrační autorita je v daný okamžik podří-

zena jediné certifikační autoritě. Certifikační autorita může mít vytvořenu pro sběr údajů a informací síť registračních autorit [Jašek 3].

3.3.2 Certifikát

Certifikát spojuje jméno držitele páru soukromého a veřejného klíče s tímto veřejným klíčem a potvrzuje tak identitu osoby. Slovy zákona o elektronickém podpisu je certifikátem „datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování podpisů s podepisující osobou a umožňuje ověřit její totožnost“. Tuto ověřenou identitu lze tedy používat nejen při podepisování dokumentů, datových souborů, ale lze ji využít také při přístupu k důvěrným nebo placeným informacím.

Výhodou certifikátů a certifikačních autorit je to, že pokud dva uživatelé věří stejné certifikační autoritě, potom výměnou certifikátů, která podepsala tato certifikační autorita, si mohou vzájemně předat a potvrdit své veřejné klíče. Tyto klíče potom mohou bezpečně používat k šifrování vyměňovaných dat a k ověřování podpisů na dokumentech.
Proces užívání certifikátu vydaného certifikační autoritou upravuje smlouva mezi uživatelem a certifikační autoritou. Tato smlouva jasně stanovuje práva a povinnosti obou smluvních partnerů. Generování digitálních certifikátů a následujícího používání je tedy placenou službou, která se musí řídit přesnými pravidly. Certifikační autorita nemůže nést odpovědnost za škody způsobené užitím certifikátu, než za kterým byl vydán. Ve smluvním vztahu jsou rovněž definována pravidla pro způsob uložení soukromého klíče, neboť právě toto uložení má na důvěryhodnost certifikátu a bezpečnost dat, chráněných takovým certifikátem, zásadní vliv [Jašek 3].

3.3.3 Další služby certifikační autority

Činnost certifikační autority ovšem nespočívá jen ve vydávání certifikátů, jejich evidenci, obhospodařování zneplatňování tak, jak nařizuje Zákon.

Mezi služby, které může certifikační autorita poskytnout patří [Jašek 3]:

- Časové razítko (Digital Time Stamp – DTS)

Časová razítka nebo časové značky ověřují, ke kterému okamžiku elektronicky podepsaný dokument existoval. Toto ověření je nesmírně důležité nejen z hlediska určení takového

okamžiku, ale i z hlediska ověření, že dokument byl podepsán v době platnosti certifikátu. Tento druhý aspekt nabývá na významu zejména pokud se taková skutečnost ověřuje po mnoha letech. Časová razítka by měla být i součástí certifikátů a údajů o jejich zneplatnění.

- Doručenky

Doručenky mají za úkol potvrdit přijetí dokumentu příjemcem. (Jde o obdobu dopisu s doručenkou, nebo potvrzení z podatelny úřadu o učiněném podání). Vzhledem k tomu, že je certifikační autorita nezávislý subjekt, může být doručenka cenným dokladem pro obě strany smluvního vztahu a v kombinace s časovým razítkem vytvořit dokonalý důkazní ověřující čas podepsání a čas doručení daného dokumentu.

- Archivační služby

Jejich úkolem je zajistit, aby archivované dokumenty bylo možné kdykoliv vyhledat a stvrdit jejich atributy způsobem přijímaným jak soukromými osobami, tak úřady státní správy. Z tohoto důvodu by nemělo jít jen o prostou archivaci dokumentů, ale o převzetí elektronických dokumentů k archivaci, při němž by došlo k ověření pravosti elektronického podpisu klienta, neporušenosti dat a připojení podpisu archivační autority s časovým razítkem. Klient by následně, a to i o velmi dlouhé době, mohl požádat archivační autoritu o vystavení potvrzení o pravosti a neporušenosti dokumentu, platnosti podpisu nebo údaje k jakému okamžiku dokument existovat. Dále by archivační autorita mohla vytvořit duplikát dokumentů v elektronické listinné podobě.

Veškeré výše uvedené služby mohou certifikační autority běžně zajišťovat už i nyní. Rozhodující pro jejich rozšíření do praxe, bude vývoj v oblasti legislativy a zájem klientů o tyto služby. Toto bude samozřejmě podmíněno nejen tím, že o této službě budou vědět, ale také jejich cenou [Jašek 3].

3.4 Důvěryhodnost poskytovatele

Velice důležitým aspektem důvěryhodnosti poskytovaných služeb je ověření důvěryhodnosti poskytovatele. V § 5 odst. 1) Vyhlášky se o datech pro vytváření kvalifikovaného elektronického podpisu poskytovatele říká, že data pro vytváření elektronického podpisu, k nimž byl vydán kvalifikovaný certifikát poskytovatele a která jsou obsažená v kvalifikovaných certifikátech poskytovatele, je poskytovatel povinen používat výhradně pro podepisování vydávaných kvalifikovaných certifikátů a seznamu zneplatněných kvalifikovaných certifikátů [13]. Pro kvalifikované certifikáty poskytovatele stanoví Vyhláška, že při zveřejňování svých kvalifikovaných certifikátů osobám spoléhajícím na certifikát je poskytovatel povinně zajistit, že jsou dostupné nejméně dvěma na sobě nezávislými způsoby [13]. Důvodem pro požadavek na zveřejnění dvěma nezávislými způsoby je možnost ověření jejich správnosti (autenticity). Předpokládá se, a praxe taková je, že držitel od poskytovatele po podpisu smlouvy o vydání kvalifikovaného certifikátu obdrží zároveň jeho kvalifikovaný certifikát.

Z uvedených skutečností vyplývá, že osoba spoléhající na certifikát opírá svou důvěru v něj o kvalifikovaný certifikát poskytovatele. Tomuto certifikátu tedy musí důvěřovat. ZoEP ani Vyhláška neupravují ověřování kvalifikovaných certifikátů poskytovatelů. Ze ZoEP však vyplývá, že důvěra ve kvalifikované certifikáty akreditovaných poskytovatelů se opírá o důvěru v Úřad, který akreditaci udělil [www 10]. Je docela pravděpodobné, že poskytovatelé certifikačních služeb budou, s cílem zvýšit svou konkurenceschopnost, uzavírat smlouvy o ověřování kvalifikovaných certifikátů, aniž by byli k tomu nuceni.

3.5 Bezpečnost

Vyhláška v § 18 odst. 4) upravuje chování poskytovatele v situaci, kdy dojde k vyzrazení dat pro vytváření elektronického podpisu poskytovatel. Vyzrazení dat pro vytváření elektronického podpisu poskytovatele je závažným bezpečnostním incidentem, při němž hrozí zneužití vyzrazených dat. Z tohoto důvodu je v takovém případě nezbytné, aby poskytovatel informaci o vyzrazení zveřejnil a zároveň zneplatnil kvalifikované certifikáty, které mohou být vyzrazením ovlivněny.

Jak ZoEP, tak Vyhláška kladou požadavky na osoby vykonávající certifikační nebo související služby. Osoby vykonávající tyto činnosti musí být odborně způsobilé a poskytovatel jim musí zajišťovat průběžná školení [13]. Odpovídající odbornost osob, které certifikační

služby zajišťují, je předpokladem jejich náležitého fungování. Odbornost je nezbytné průběžně zvyšovat formou školení. Bezpečnostní vědomí je uvědomění si všech aspektů bezpečnosti při poskytování certifikačních služeb a uzpůsobení vlastního chování tak, aby byla stanovená úroveň bezpečnosti dodržována. Jedná se o činnosti, na které jsou z hlediska náležitého fungování certifikačních služeb kladeny zvýšené nároky a u kterých selhání osoby při jejich výkonu má vliv na informační bezpečnost. Účastníci elektronické komunikace s využitím elektronického podpisu musí mít záruku, že tyto činnosti vykonávají osoby, které jsou důvěryhodné. Absence záznamu v rejstříku trestů je jedním z výrazů důvěryhodnosti.

4 VYUŽITÍ ELEKTRONICKÉHO PODPISU V KOMUNIKACI S VEŘEJNOU SPRÁVOU

Existence zákona, který obsahuje základní právní podmínky pro vytváření a používání elektronického podpisu v České republice, umožnila současně i přípravu některých základních předpisů pro aplikaci tohoto zákona v oblasti veřejné správy. Proto bylo v návaznosti na zákon o elektronickém podpisu přijato nařízení vlády č. 304/2001 Sb., kterým se provádí zákon 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů. Jeho obsahem je právní úprava základních organizačně technických opatření orgánů veřejné moci včetně územních samosprávných celků provádějících výkon státní správy v rámci přenesené působnosti. Těmito opatřeními bude zabezpečena povinnost těchto orgánů přijmout podání učiněné v elektronické podobě a podepsané elektronicky, bude-li toto právo orgánům veřejné moci stanoveno zvláštním předpisem. Pro orgány veřejné moci toto nařízení současně stanoví povinnost zřídit pro příjem a odesílání datových zpráv pracoviště splňující požadavky na technické a programové vybavení podle standardu vydaných Úřadem pro veřejné informační systémy a umožňující používání zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb.

4.1 Komunikace s veřejnou správou

Chodit na úřady a vyplňovat různé formuláře, způsobuje většině značné problémy. Téměř neřešitelným problémem jsou pro zaneprázdněného občana úřední hodiny. Dá se návštěva úřadů tedy vyřešit způsobem odpovídajícím současným životním trendům? Nepotrvá to tak dlouho a spojení s úřady bude daleko jednodušší. Komunikovat s úředníky budeme moci, aniž bychom přitom opustili svůj byt anebo kancelář. Dálkový, nebo-li elektronický přístup k informacím prostřednictvím počítače a Internetu v jednodušší podobě už ale nyní funguje. To znamená, že s většinou úřadů, zejména samosprávy, je možné komunikovat v takové té jednoduché podobě „dotaz – odpověď“. Lze očekávat, že se to velmi brzo začne vyvíjet k dalším kvalitativním stupňům, neboť se buduje tzv. intranet veřejné správy, což je speciální komunikační síť pro datové přenosy, která bude mít veškeré prvky moderního zabezpečení. Ta vytvoří, spolu s již existujícím elektronickým podpisem, jakési technické zázemí pro to, aby bylo možné komunikovat s úřadem už nejenom tou formou „dotaz – odpověď“, ale skutečně elektronicky získávat určité úřední výkony, to znamená různá

potvrzení, rozhodnutí atd. Tímto tedy odpadne osobní cesta na úřad a také jednání s úředníky a nakonec i ono dodržování úředních hodin. Dokumenty takto získané budou mít ovšem stejnou právní platnost jako při návštěvě osobní. K tomuto ovšem bude potřeba ještě upravit některé legislativní normy, které zatím s touto možností nepočítají. Půjde o zrovnoprávnění předávání dokumentů elektronickou formou s tou dosud existující a známou papírovou formou. Legislativa by také měla zajistit to podstatné pro každého občana, a to vyloučit pochybnosti o tom, jestli správní úkon byl učiněn opravdu tím, kdo je k němu oprávněn, a byl učiněn správně.

Stejně tak jako elektronická komunikace občan – úřad bude v budoucnu fungovat i elektronické spojení úřad – úřad. Právě elektronická komunikace mezi úřady navzájem velmi zrychlí a také podstatně zkvalitní řadu správních úkonů. Jednoduše řečeno, už nebude potřeba navštěvovat jeden úřad za druhým, ale v podstatě z jednoho místa, z jednoho úřadu bude možné teoreticky vyřídit celou agendu příslušného správního úkonu.

4.2 Připravovaná řešení

Veřejná správa se musí tedy připravit na novou generaci občanů, která bude schopna z časových důvodů komunikovat pouze elektronicky. Přinese to samozřejmě pozitiva i do úřadu: ubude vyzvánějících telefonů, přenášení papírů atd. To zvýší operativnost a výkonnost úředníků a v neposlední řadě sníží náklady. Microsoft v této souvislosti nabízí tři typy technologie e-governmentu (elektronizace veřejné správy), a to portál veřejné správy, digitální komunity a systémy elektronické veřejné správy [5].

4.2.1 Portál veřejné správy

Jedná se o přístupové místo občanů k veřejné správě, a to elektronickou cestou. Cílem tohoto projektu je vytvoření virtuálního úřadu na bázi elektronické správy, tzv. e-government. Prostřednictvím portálu budou z jednoho referenčního bodu přístupny věrohodné a aktuální informace z veřejné správy ČR. Uživatelé tak budou moci s úřady komunikovat rychle a efektivně. Měl by nám umožnit získat co nejvíce informací o tom, co se kde, jak a za kolik vyřizuje. Znamená to, že by občan měl nalézt informace o jednotlivých institucích veřejné správy a o postupech při vyřizování konkrétních úředních záležitostí. Zde by mohl také nalézt příslušné formuláře a případně si je i elektronicky s úřady vymě-

nit. Při příležitosti využívání portálu se mohou občané zúčastnit i různých průzkumů veřejného mínění, zapojit se do politických diskusí.

4.2.2 Digitální komunity

Jednotlivcům jsou nejblíže místní, komunální složky veřejné správy. Obecní úřady přicházejí do styku s většinou klíčových událostí v životě lidí – registrují nové občánky, vykonávají sňatky atd.. Tento základní vztah mezi občanem a obecním úřadem se v informační epoše nezmění. Informační technologie mohou však tento vztah zkvalitnit, propojit místní instituce dohromady a vytvořit „digitální komunity“, propojit státní správu, občany, podniky, školy a kulturní instituce.

4.2.3 Systémy elektronické veřejné správy

Tyto systémy pomohou státu propojit portál veřejné správy, místní digitální komunity a široké spektrum služeb a funkcí veřejné správy do jednotného celku.

Existence Internetu mění celou společnost, a tím také veřejnou správu, která se stává postupně „elektronickou veřejnou správou“. Internet je dostupný stále většímu počtu občanů, kteří vyžadují pohodlnější elektronický přístup k veřejným službám. Na druhou stranu si úřady uvědomují, že díky využívání Internetu mohou významně zkvalitnit své služby a snížit náklady.

II. PRAKTICKÁ ČÁST

5 ELEKTRONICKÁ KOMUNIKACE S DAŇOVOU SPRÁVOU

Prostředí Internetu a jeho dostupnost stále širšímu okruhu občanů a organizací vytváří příznivé podmínky pro využití elektronické komunikace v běžném životě každého z nás. Existence Internetu mění celou společnost, a tím také státní správu, která se stává „elektronickou státní správou“ (e-government). Internet je dostupný stále většímu počtu občanů, kteří vyžadují pohodlnější elektronický přístup k veřejným službám. Na druhou stranu si úřady uvědomují, že díky využívání Internetu mohou významně zkvalitnit své služby a snížit náklady. Jde o přínos zejména v zavádění elektronické komunikace mezi občanem - daňovým poplatníkem, resp. plátcem (daňovým subjekt), a daňovou správou Ministerstva financí České republiky.

Co konkrétně e-government v oblasti daní pro občana či organizaci znamená? Stručně řečeno, jde o to plnohodnotně nahradit výměnu listinných dokumentů, spojenou s jejich fyzickým přeposíláním mezi občanem a finančním úřadem, určitým elektronickým mechanizmem, a to prostřednictvím veřejné datové sítě Internet. Aby náhrada byla skutečně plnohodnotná, musí mít tento mechanizmus řadu vlastností, jako např. jsou:

- Elektronický dokument obsahuje úplnou informaci, má přesně definovanou strukturu a význam jednotlivých datových položek.
- Údaje o struktuře a významu položek elektronických daňových podání jsou v plném rozsahu veřejné, takže další firmy vytvářející např. software pro podporu účetnictví mohou jejich automatizovanou tvorbu zahrnout do svých produktů.
- Elektronický dokument je důvěryhodný, tj. buď podepsaný zaručeným elektronickým podpisem podle ZoEP nebo jinak kryptograficky ochráněn proti neautorizovanému vytvoření či změně.
- Při transportu přes prostředí internetu je důvěrnost dokumentu (tj. zabezpečení proti přečtení) ochráněna šifrováním.
- Zaslání dokumentu jednou stranou musí být druhou stranou elektronicky potvrzeno, a toto potvrzení musí být v potřebné míře nezpochybnitelné a musí být uloženo pro případné pozdější řízení.

- Na straně občana či organizace by práce s daňovým elektronickým dokumentem neměla vyžadovat žádné speciální investice nad rámec běžného vybavení, jež je pro připojení k internetu nutné (počítač, připojení k síti, internetový prohlížeč).

Možnost podání písemností pro daňovou správu v elektronické podobě je zpracováno v souladu s platnou legislativou zejména se zákonem č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů, zákonem č. 227/2000 Sb., o elektronickém podpisu, ve znění pozdějších předpisů a metodickým pokynem D-252.

Dne 1. července 2002 vstoupila v platnost novela zákona č. 337/1992 Sb., o správě daní a poplatků, která mimo jiné upravuje elektronickou formu komunikace mezi daňovými subjekty a jejich správci daně. Tímto skončilo faktické právní vakuum, které (mimo mnoha jiných faktorů) dosud bránilo plnému využití možností, které elektronický podpis nabízí. Novela má „tu moc" zjednodušit a zrychlit agendu, která souvisí s podáním daňových přiznání všech možných typů. Snahou zákonodárců přitom bylo aplikovat elektronický podpis na celou oblast správy daní.

Ministerstvo financí v souladu s platnou legislativou připravilo pro daňové subjekty možnost podávat daňové přiznání a další písemnosti v elektronické podobě. Podání lze uskutečnit jako podání s datovou zprávou opatřenou zaručeným elektronickým podpisem nebo jako podání s datovou zprávou neopatřenou zaručeným elektronickým podpisem.

Daňová správa Ministerstva financí České republiky uvedla již začátkem roku 1993 do provozu Automatizovaný Daňový Informační Systém (dále jen „ADIS"), který je od počátku koncipován jako ucelená počítačová podpora celého spektra činností spojených se správou daní podle příslušné legislativy. Je proto logické umožnit občanům a organizacím využít potenciál výpočetní techniky pro přímou elektronickou komunikaci s finančním úřadem, usnadnit jim mnohdy značně obtížné ruční vyplňování daňových přiznání a v neposlední řadě uvolnit kapacitu pracovníků daňové správy směrem od ručního pořizování dat z listinných dokumentů k automatizovanému daňovému řízení s použitím zkontrolovaných autorizovaných elektronický dat.

Správa konkrétní daně pro určitého občana či organizaci je podle zákona o správě daní a poplatků vždy místně příslušná ke konkrétnímu finančnímu úřadu (FÚ), resp. konkrétnímu správci daně, který daně spravuje s podporou automatizovaného systému „ADIS". Při klasické listinné komunikaci je občan v kontaktu s tímto lokálním správcem daně a pouze ve

speciálních případech (např. odvolání) vstupuje do hry vyšší orgán, finanční ředitelství (FŘ) nebo Ústřední finanční a daňové ředitelství (ÚFDŘ). Autorizace listinných podání se děje formou klasického podpisu, který však za nepřítomnosti subjektu nelze ověřit, protože daňová správa neeviduje podpisové vzory.

5.1 Elektronické podatelny

Nástrojem elektronické komunikace mezi občanem a úřady jsou podle nařízení vlády elektronické podatelny. Elektronická podatelna je zpravidla založena na komunikaci prostřednictvím elektronické pošty nebo prostřednictvím webových technologií. Z pohledu občana se může zdát e-mailová komunikace jednodušší a přirozenější, často ovšem přináší problémy. Obtížně se zde kontroluje, zda občan dokument vyplnil a jestli jej správně elektronicky podepsal.

V případě elektronické komunikace, tj. podávání daňových přiznání subjektem prostřednictví internetu, je situace v řadě podstatných aspektů odlišná. První odlišností je, že subjekt nekomunikuje se svým lokálním FÚ, ale s technickým zařízením na ÚFDŘ, které zákon o správě daní a poplatků označuje jako tzv. společné technické zařízení správců daně.

5.2 Postup při elektronickém podání

Technické zařízení na ÚFDŘ automatizovaně poskytuje následující služby:

1. Dává k dispozici specializovanou aplikaci pro elektronická podání (dále jen EPO), kterou si subjekt spustí ve svém internetovém prohlížeči.
2. Umožní vyplnit nebo převezme a zkontroluje daňové podání zaslané subjektem. Veškeré zpracování probíhá na PC poplatníka bez odesílání jakýchkoli citlivých údajů. Kontroly daňových přiznání berou v úvahu nejen požadavky příslušného tiskopisu, ale i algoritmus všech kontrol, které na skutečném přiznání provádí správce daně (včetně kontrol na číselníky, jako např. seznam katastrálních území, platné sazby atd.). Zkontrolované podání má subjekt možnost odeslat on-line na společné technické zařízení správců daně.
3. Při příjmu podání je zkontrolován zaručený elektronický podpis, provedou se kontroly správnosti struktury písemností a podání je uloženo do centrálního bezpečného úložiště. V rámci trvajícího spojení s prohlížečem daňového subjektu mu technické

zařízení odešle elektronické potvrzení přijetí s časovou známkou, která má stejnou právní účinnost, jakou má v případě listinných podání potvrzení podatelny FÚ nebo České pošty.

4. Je-li podání odmítnuto, a to z důvodu neprůchodnosti přes nepropustné kontroly – např. neplatnost zaručeného elektronického podpisu, neplatný formát souboru, absence povinných údajů aj., subjekt obdrží dokument o nalezených chybách.

5. Je-li podání přijato, předá je společné technické zařízení správců daně po síti Finet-ADIS (privátní síť daňové správy ČR pro komunikaci mezi FÚ, FŘ a ÚRDŘ) k dalšímu zpracování na FÚ, kde je nahráno do lokální databáze „ADIS“ analogicky, jako kdyby bylo pořízeno ručním typováním.

Společné technické zařízení správci daně umožňuje převzít soubor s podáním, který byl vytvořen i jinou aplikací třetí strany – např. účetní či daňové systém, jeho struktura i obsah musí splňovat zveřejněnou dokumentaci. Stejně jako v případě aplikace EPO toto zařízení elektronicky potvrdí, resp. odmítne zaslaný soubor.

6 ELEKTRONICKÉ DAŇOVÉ ŘÍZENÍ

Aplikace EPO může být provozována buď v on-line režimu, tj. za stálého spojení s WWW serverem společného technického zařízení správců daně, nebo v off-line režimu (bez spojení). V obou případech se může rozpracovaný soubor podání uložit na lokálním počítači a vlastní odeslání je možno učinit kdykoliv později. Aplikace EPO v případě potřeby automaticky stahuje při práci potřebné číselníky či jejich části. Před odesláním dokumentu provádí všechny kontroly, a to tytéž jako společné technické zařízení správců daně na ÚFDŘ. Při použití aplikace EPO by se nemělo stát, že již jednou lokálně zkontrolované podání bude v centru odmítnuto. Aplikace může pracovat ve dvou základních režimech [www 7]:

- bez elektronického podpisu,
- se zaručeným elektronickým podpisem – tzn., že fyzická osoba, která zprávu podepsala, nemůže popřít, že je původcem této zprávy (nepopiratelnost), je možné zjistit, zda zpráva nebyla změněna poté, co byla podepsána (zachování integrity), je možné zjistit identitu podepsané osoby a je zajištěna právní akceptovatelnost podpisu.

6.1 Elektronické podání bez zaručeného elektronického podpisu

V případě podání s datovou zprávou neopatřenou zaručeným elektronickým podpisem se ještě vyžaduje podání v písemné podobě, tj. doručení počítačové sestavy správci daně (e-tiskopis). Tyto počítačové sestavy mají údaje, obsah i uspořádání údajů zcela totožné s tiskopisy daňového přiznání. E-tiskopis daňového přiznání je vytisknut uvedeným programem až po zpracování daňového přiznání a po uložení na disketu nebo po odeslání prostřednictvím sítě Internet.

6.1.1 Podání prostřednictvím sítě Internet

Byla-li při podání daňového přiznání odeslána datová zpráva prostřednictvím sítě Internet, je za den podání daňového přiznání považován den, kdy byl e-tiskopis daňového přiznání, při splnění ostatních podmínek pro podání, podán správci daně. Bude-li podání datové zprávy prostřednictvím sítě Internet učiněno ve lhůtě pro podání, přičemž e-tiskopis daňového přiznání bude podán ve lhůtě 3 dnů po lhůtě pro podání, správce daně bude s ohledem

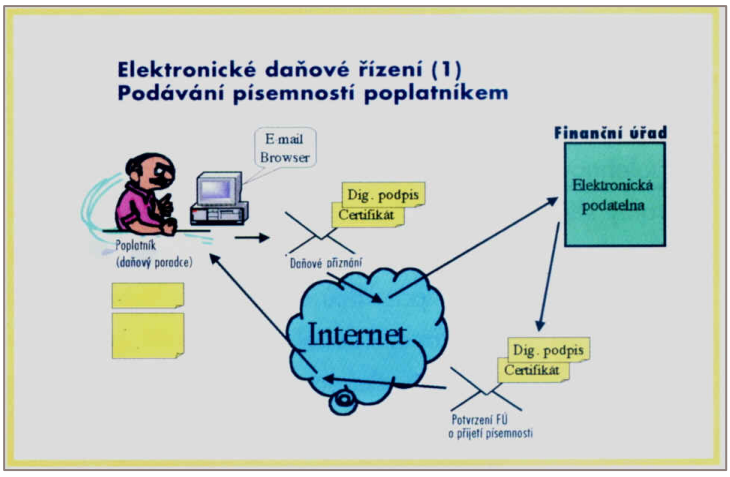
na výhody, které pro něj vyplývají z elektronického doručení daňového přiznání, postupovat stejně, jako kdyby dnem doručení e-tiskopisu daňového přiznání byl den přijetí datové zprávy na společné technické zařízení správců daně. V tomto případě se běh lhůt odvíjí od data doručení e-tiskopisu.

6.1.2 Podání prostřednictvím diskety

Byla-li při podání daňového přiznání datová zpráva podána na disketě, je za den podání daňového přiznání považován den, kdy byly e-tiskopis daňového přiznání a disketa, za splnění ostatních podmínek pro podání, podány správci daně [pokyn D-252 15].

6.2 Elektronické podání opatřené zaručeným elektronickým podpisem

V případě podání učiněném prostřednictvím datové zprávy, opatřené zaručeným elektronickým podpisem, musí být subjekt vybaven platným kvalifikovaným certifikátem a k němu příslušným privátním klíčem, kterým dokument před odesláním podepíše (v rámci aplikace EPO). Veškerá komunikace je výlučně elektronická a subjekt na FÚ nepodává žádné listinné dokumenty.



Obr. 2. Komunikace poplatníka s finančním úřadem prostřednictvím internetu.

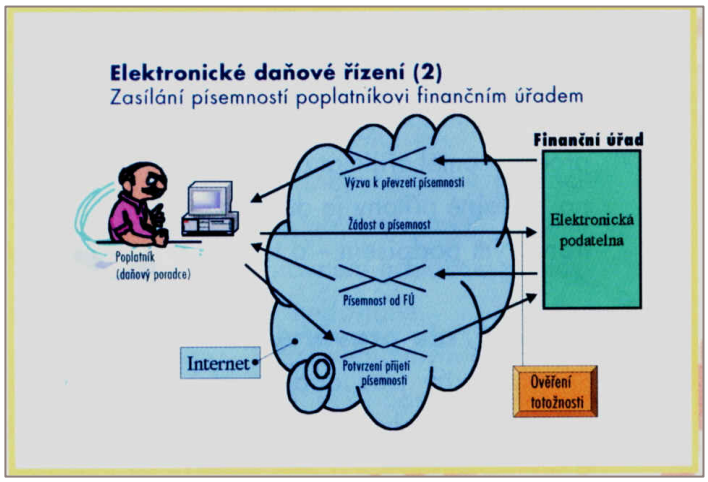
Obrázek (Obr. 2) zobrazuje komunikaci s finančním úřadem, kdy je podání učiněno pomocí internetu. Potřebné funkce jsou zabezpečeny prostřednictvím www aplikace poskytnuté elektronickou podatelnou [11].

6.2.1 Elektronické potvrzení o přijetí

Elektronické potvrzení o přijetí vystaví elektronická podatelna a je zasláno zpět poplatníkovi. V obou výše uvedených případech podání je potvrzení společného technického zařízení správců daně sice elektronicky podepsáno (privátním klíčem příslušným k certifikátu tohoto zařízení, který byl vystaven interní certifikační autoritou daňové správy), ale nikoliv zaručeným elektronickým podpisem ve smyslu ZoEP, tzn., že podpis je vytvářen automatizovaně technickým zařízením bez kontroly podepisující fyzické osoby. Platnost tohoto dokumentu je srovnatelná s platností podacího lístku pošty.

6.2.2 Zaslání daňové písemnosti poplatníkovi

Elektronické daňové řízení, při kterém je správce daně iniciátorem (jde např. o zaslání daňové písemnosti poplatníkovi), je komplikovanější, protože poplatník samozřejmě nemusí být trvale on-line připojen (na rozdíl od FÚ) k síti. Předpokládá se, že napřed FÚ vyšle e-mailem výzvu poplatníkovi, že tento má na elektronické podatelně připravenou písemnosti k vyzvednutí. Poplatník, že obdržel výzvu, se připojí k serveru podatelny FÚ, zašle mu podepsanou žádost – písemnost (kvůli ověření své totožnosti vůči FÚ) a v rámci téhož připojení písemnost podepsanou správcem daně převezme. Příslušný program pak automaticky potvrdí FÚ přijetí písemnosti poplatníkem prostřednictví podepsaného potvrzení přijetí písemnosti, tj. vystaví a na podatelnu FÚ odešle jím podepsanou „elektronickou doručenku“. Protože není na 100 % zaručeno, že poplatník výzvu e-mailem skutečně obdrží (např. chybná e-mail adresa, porucha sítě, poplatník se delší dobu nepřipojil k síti atd.), je možné např. výzvu zaslat elektronicky 3x, a pokud není elektronická písemnost ve stanovené lhůtě vyzvednuta, lze ji pak poslat klasicky poštou jako listinný dokument – na doručenku.



Obr. 3. Komunikace při elektronickém doručování poplatníkovi.

Obrázek (Obr. 3) nám zobrazuje komunikaci elektronického doručování poplatníkovi. Potřebná realizace je docílena pomocí kombinace elektronické pošty zaslané poplatníkovi („Výzva k převzetí písemnosti“), a www aplikace podatelny, která následně poplatníkovi umožní písemnost převzít (samozřejmě proti prokázání totožnosti a potvrzení převzetí) [10].

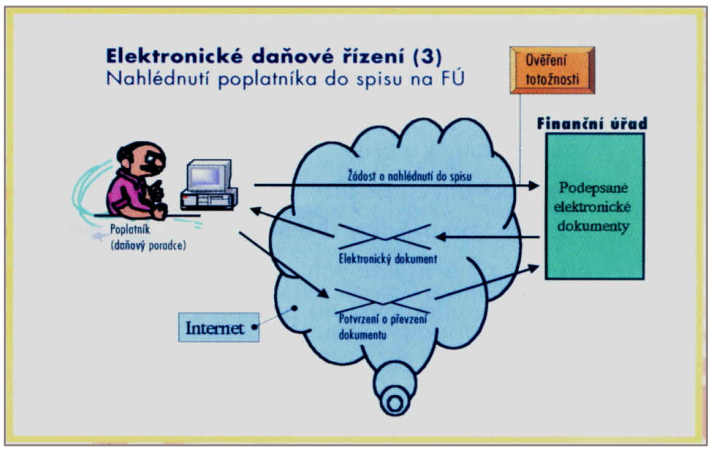
7 PRAKTICKÁ REALIZACE BEZPEČNÉ KOMUNIKACE S DAŇOVOU SPRÁVOU

Podobně jako klasické listinné dokumenty je třeba archivovat i elektronické dokumenty. Archiv zejména garantuje, že se dokument neztratí, že nebude změněn a že se nedostane do nepravých rukou. Elektronické dokumenty mají navíc výhodu v tom, že je lze snadno kopírovat. Jednotlivé kopie pak mohou být uloženy na geograficky vzdálených pracovištích archivu. Tím může předejít ztrátě dokumentu při živelních pohromách nebo při válečných konfliktech.

Nevýhodou elektronických dokumentů je, že jsou uloženy na médiích, která stárnou podstatně rychleji než papírové dokumenty. Elektronické dokumenty se pak musí v archivu pravidelně obnovovat kopírováním na čerstvá média.

U elektronicky podepsaných dokumentů je ještě další problém, kterým je „efekt vyprchávání“ elektronického podpisu. Elektronický podpis má ještě kratší možnost ověřování než podpis na papírovém dokumentu. Je přesně vymezen platností certifikátu určeného pro ověření podpisu.

Vzhledem k tomu, že dalším důležitým institutem daňového řízení je právo poplatníka nahlédnout do svého spisu, je možné též uvažovat o jeho elektronické podobě, především s výhledem na dálkový přístup. Je samozřejmé, že elektronické nahlédnutí do spisu se může týkat pouze písemností archivovaných v elektronické podobě a tudíž plně nerealizuje klasické nahlédnutí. Elektronické nahlédnutí do spisu bude opět začínat žádostí podepsanou poplatníkem (ověření totožnosti tazatele), přes vlastní odeslání požadovaných dat ze serveru FÚ až po přijetí potvrzení na FÚ o jejich převzetí poplatníkem.



Obr. 4. Komunikace při nahlédnutí poplatníka do elektronického spisu.

Obrázek (Obr. 4) nám zobrazuje komunikace při nahlédnutí poplatníka do elektronického spisu s dálkovým přístupem. Potřebná funkcionalita výše uvedené možnosti je zabezpečena například pomocí www aplikace, která poplatníkovi umožní vyplnit formulář s žádostí, elektronicky tuto žádost podepsat, a po kontrole odeslat [11].

8 ANALÝZA VYUŽITÍ ELEKTRONICKÉHO PODÁNÍ DAŇOVÝCH PŘIZNÁNÍ

V této části jsem se pokusila udělat u veřejnosti díky dotazníku průzkum a na základě získaných výsledků vyhodnotit využívání elektronického podání daňových přiznání. Před rozesláním dotazníků daňovým poradcům a účetním zpracovávající daňové přiznání, byla má domněnka taková, že se elektronické podání daňových přiznání u nás oblibě příliš netěší. Proč? Zřejmě z toho důvodu, že je k němu potřeba vlastnictví, pro někoho drahého, elektronického podpisu. Kdyby se ten z celého procesu vypustil, jistě by počet lidí komunikujících s daňovou správou on-line vzrostl.

Podávat daňová přiznání prostřednictvím internetu může mít řadu výhod. Přiznání k jednotlivým daním má v dnes běžném provedení vždy podobu formuláře s předem definovanými řádky, které je nutné podle metodického návodu vyplnit. Jeho převedení do podoby www stránky na internetu nebo jednoduchého programu by nemuselo nic bránit. Obecně řečeno každou komunikaci mezi občanem a státem, která se odehrává s pomocí formuláře, je možné poměrně snadno přenést do elektronické (počítačové) podoby. Aby taková komunikace fungovala, musí na ni být v prvé řadě obě strany připraveny. Současně musí být taková výměna informací co nejjednodušší a musí zachovávat přiměřenou úroveň bezpečnosti.

Podávat daňová přiznání by mohlo být stejně jednoduché jako obsluha bankovního účtu prostřednictvím internetového bankovnictví. Poplatník by takovou aplikaci mohl využít, i když by byl služebně mimo místo svého podnikání, třeba i v noci či o víkendu. Výhodou elektronických formulářů daňových přiznání je i to, že mohou obsahovat kontrolní mechanizmy pro odhalení překlepů a špatných výpočtů. Když si k tomu přidáme fakt, že elektronicky a na dálku by bylo možné podávat přiznání ke všem typům daní, objeví se otázka, proč se elektronická podávání daňových přiznání rozšiřují tak pomalu. Odpověď, se domnívám, je v celku jednoduchá – bez certifikátu se nepřiznáte.

Dotazník jsem zaměřila, jak jsem již uvedla, především na daňové poradce a na účetní zpracovávající daňové přiznání, protože se myslím, že využití elektronického podání se stále vyplatí více tomu, kdo s finančním úřadem komunikuje častěji, tedy podává daňové přiznání za více poplatníků a na více daních (daň z příjmu, daň z přidané hodnoty, silniční daň).

8.1 Praktické zpracování dotazníků

Dotazníky byly rozeslány v regionu Bystřice pod Hostýnem, Holešova, Přerova a Hranic, to v celkovém počtu 100 ks.

Zjištěné hodnoty jsou uvedeny v tabulce (Tab. 1).

Hodnoty	%	ks
Vrácené dotazníky	70	70
Nevrácené dotazníky	30	30
Celkem	100	100

Tab. 1. Celkový počet rozeslaných dotazníků

Graf 1. Celkový počet rozeslaných dotazníků

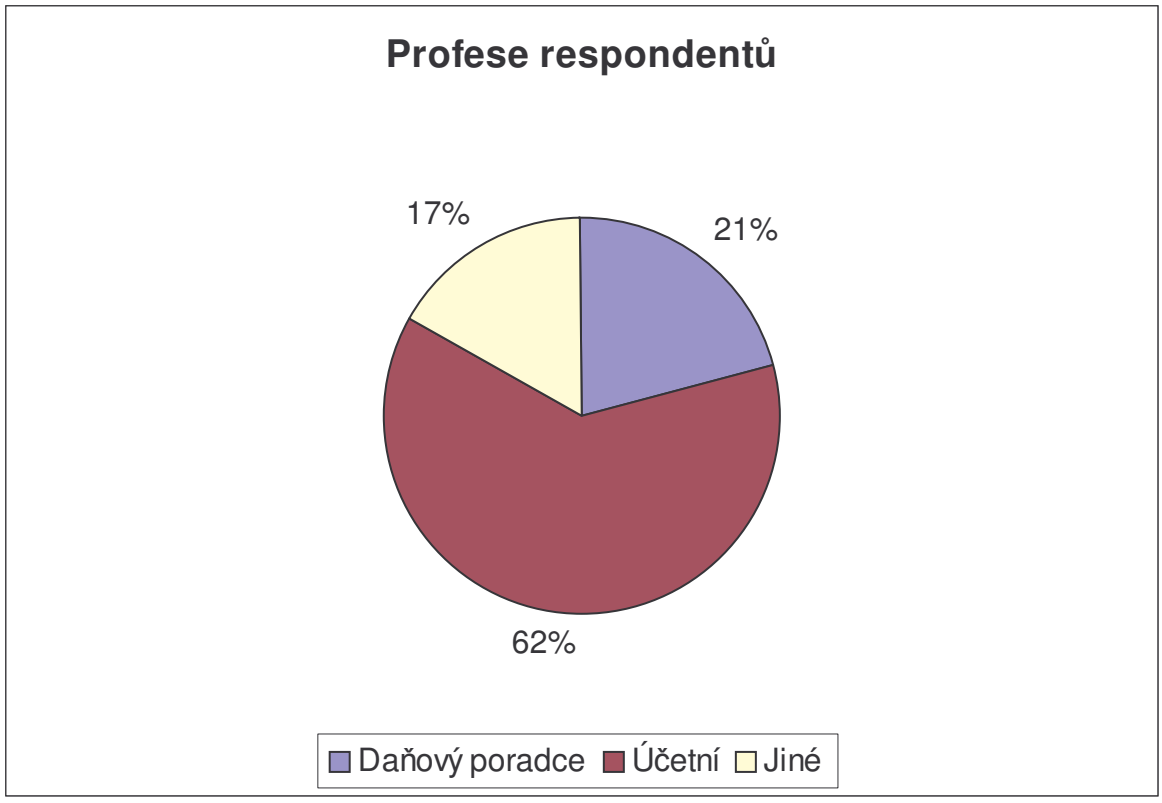
V dalším zpracování budu tedy vycházet z celkového počtu vrácených dotazníků, tedy 70 ks.

Dotaz č. 1: **Profese respondentů**

Zjištěné hodnoty jsou uvedeny v tabulce (Tab. 2.

Hodnota	%	Počet
Daňový poradce	21	15
Účetní	62	43
Jiní	17	12

Tab. 2. Profese respondentů



Graf 2. Profese respondentů

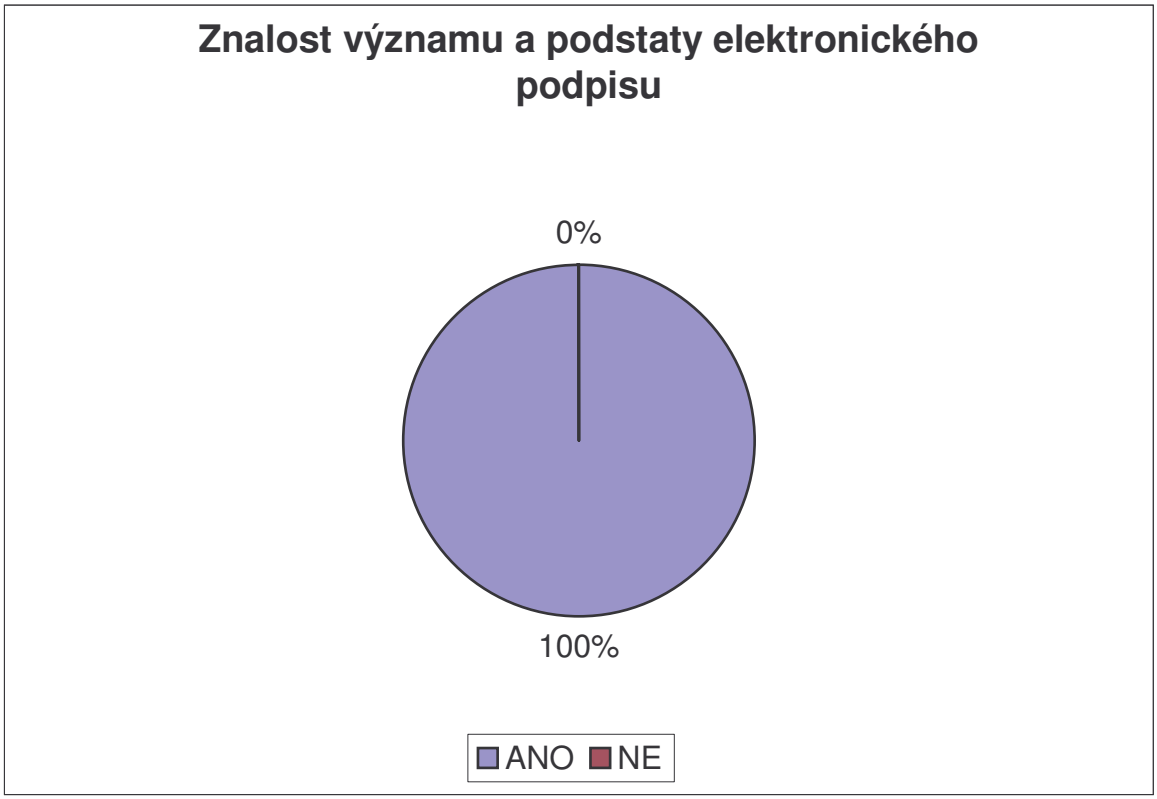
Mezi dotazovanými byla většina daňových účetních, a to v počtu 62 %, daňoví poradci se podíleli na vyplnění dotazníků 21 % a jiní, mezi které spadají především osoby samostatně výdělečně činné, 17 %.

Dotaz č. 2: **Znáte význam a podstatu elektronického podpisu?**

Zjištěné hodnoty jsou uvedeny v tabulce (Tab. 3).

Možné odpovědi	%	počet
ANO	100	70
NE	0	0

Tab. 3. Znalost významu a podstaty elektronického podpisu



Graf 3. Znalost významu a podstaty elektronického podpisu

Na základě zjištěných odpovědí, můžu jednoznačně konstatovat, že význam a podstata elektronického podpisu je veřejnosti známa, nebo se alespoň respondenti domnívají, že ví, jaké jim elektronický podpis nabízí možnosti, výhody popř. nevýhody.

Dotaz č. 3: **Využíváte možnosti elektronického podání daňového přiznání?**

Zjištěné hodnoty jsou uvedeny v tabulce (Tab. 4).

Možné odpovědi	%	Počet
ANO	28	20
NE	72	50

Tab. 4. Využití elektronického podání daňového přiznání

Graf 4.Využití elektronického podání daňového přiznání

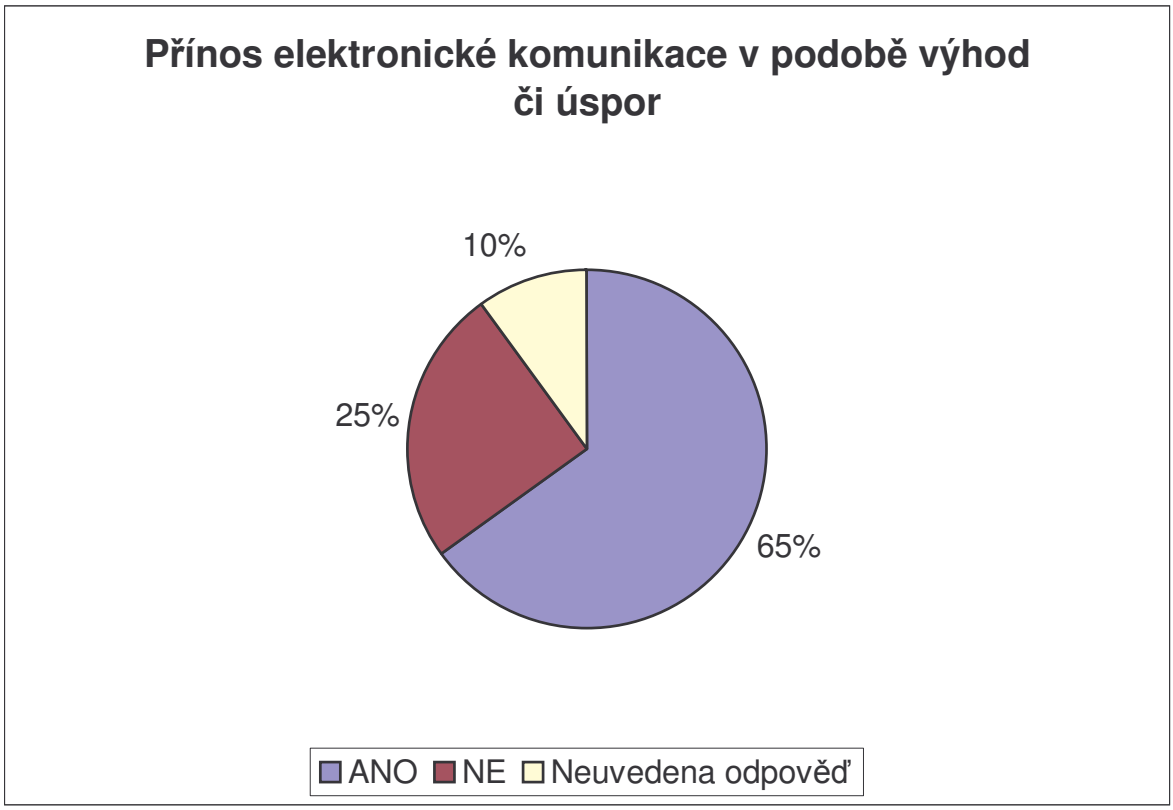
Z výše uvedeného výsledku je zřejmé, že elektronického podání využívá pouze 72 % dotazovaných. Zjistila jsem, že se jedná téměř o všechny dotazované daňové poradce. Domnívám se, že právě této „skupině“ se nejvíce vyplatí investovat do koupi kvalifikovaného certifikátu, s jehož použitím pak následně mohou daňoví poradci přiznání svých klientů před odesláním na finanční úřad elektronicky podepisovat.

Dotaz č. 4: **Přináší Vám využití elektronické komunikace jisté výhody nebo úspory?**

Zjištěné hodnoty jsou uvedeny v tabulce (Tab. 5).

Možné odpovědi	%	Počet
ANO	65	13
NE	25	5
Neuvedena odpověď	10	2
Celkový počet odpovědí		20

Tab. 5. Přínos elektronické komunikace v podobě výhod či úspor



Graf 5. Přínos elektronické komunikace v podobě výhod či úspor

Tato otázka navazovala na odpověď otázky předchozí, tedy odpovídat měl pouze ten, kdo možnosti elektronické komunikace s daňovou správou využívá. 20 respondentů uvedlo, že využívá této možnosti, 65 % řináší elektronická komunikace výhody, v dotazníku všichni

takto odpovídající uvedli výhodu především v časové úspoře. Ostatních 25 % v této možnosti podání nevidí žádné výhody ani úspory, ale přesto s finančními úřady elektronicky komunikují. 10 % respondentů žádné výhody ani úspory neuvedlo.

Dotaz č. 5: **Znáte konkrétní společnost, která Vám umožní získat zaručený elektronický podpis? V případě, že ano, uveďte její název.**

Zjištěné hodnoty jsou uvedeny v tabulce (Tab. 6).

Možné odpovědi	%	Počet
ANO	64	45
NE	36	25

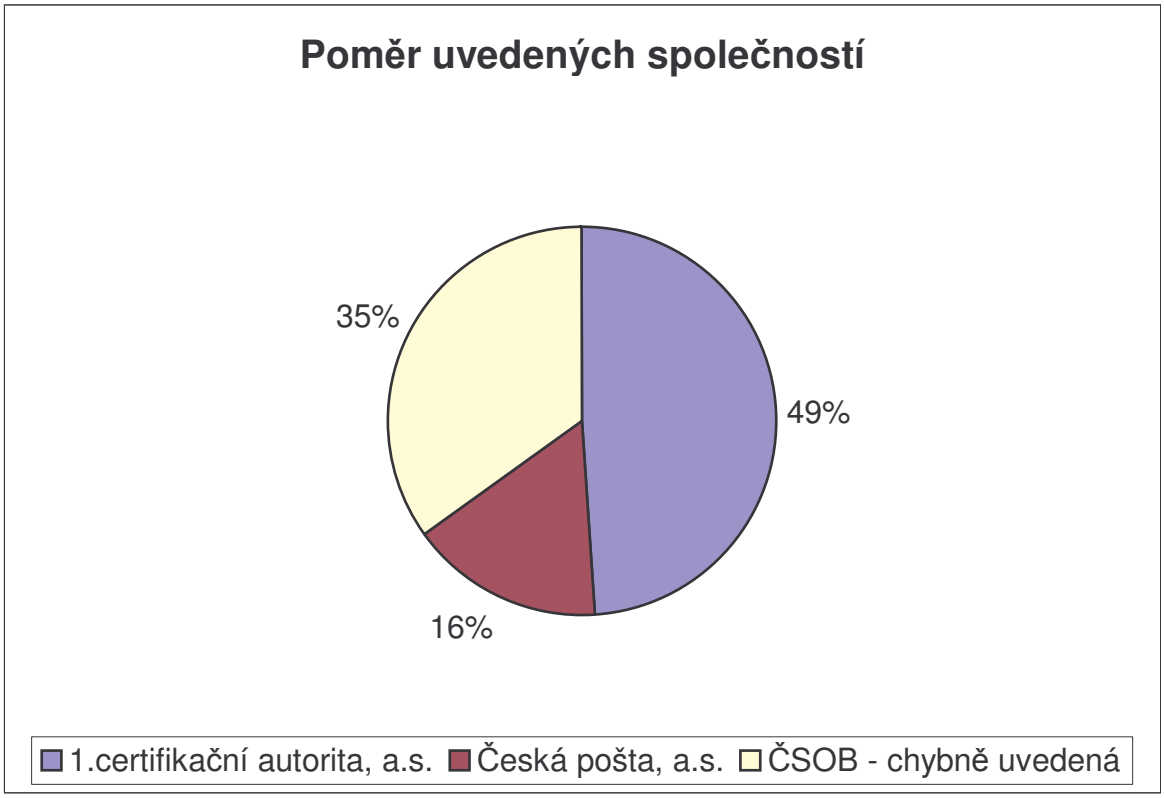
Tab. 6. Znalost konkrétní společnosti poskytující ZAREP

Graf 6. Znalost konkrétní společnosti poskytující ZAREP

Názvy uvedených společností, které poskytují elektronický podpis, jsem uvedla do tabulky (Tab. 7).

Názvy společností	%	Počet
1.certifikační autorita, a.s.	49	22
Česká pošta, a.s.	16	7
ČSOB - chybně uvedená	35	16

Tab. 7. Názvy uvedených společností



Graf 7. Poměr uvedených společností

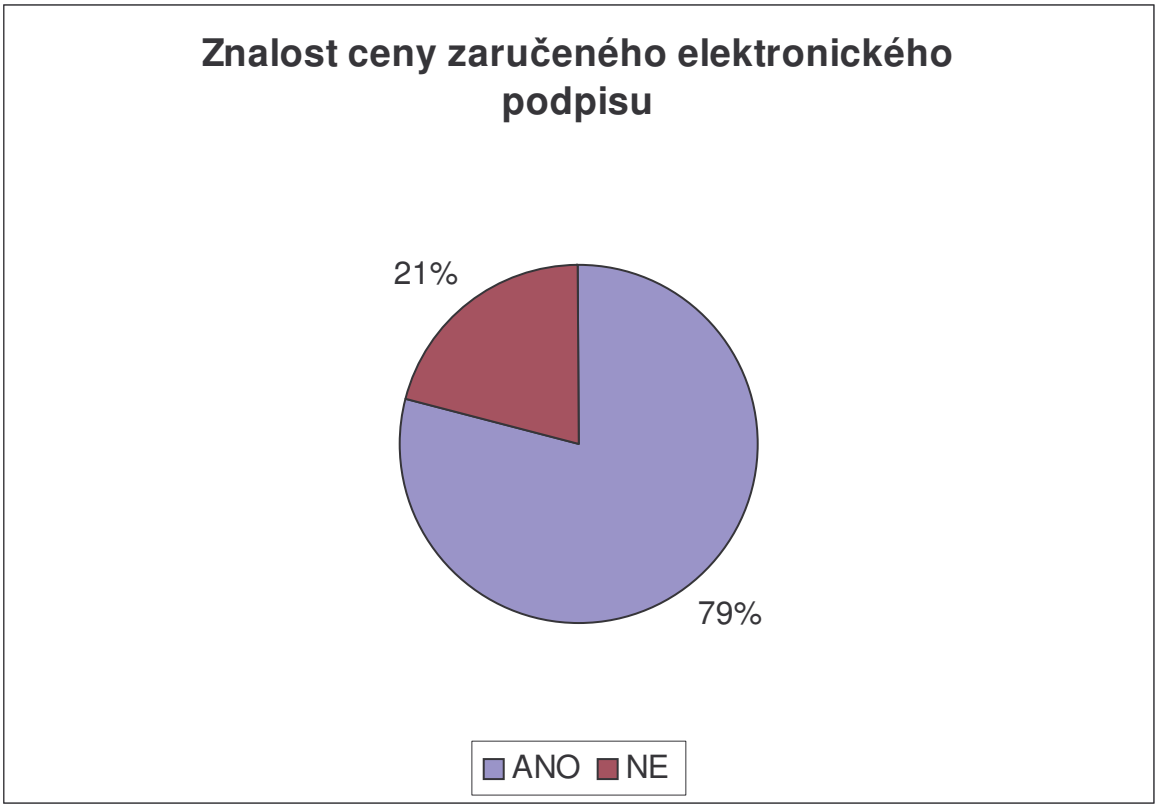
Z předchozího grafu je zřejmé, že 64 % odpovídajících zná konkrétní společnost poskytující elektronický podpis, nebo se aspoň domnívá, že zná. V odpovědích se nejčastěji objevovaly následující společnosti: Česká pošta, a.s., 1. certifikační autorita a společnost ČSOB. ČSOB ovšem dotazovaní uváděli mylně, jelikož tato společnost může elektronický podpis vydávat zase jen prostřednictvím 1. certifikační autority. Poměr uvedených společností je pro přehlednost opět zobrazen v grafu.

Dotaz č. 6: **Je Vám známa cena pořízení zaručeného elektronického podpisu?**

Zjištěné hodnoty jsou uvedeny v tabulce (Tab. 8).

Možná odpověď	%	Počet
ANO	79	55
NE	21	15

Tab. 8. Znalost ceny ZAREP



Graf 8. Znalost ceny ZAREP

79 % odpovídajících je známa cena zaručeného elektronického, 21 % nikoliv.

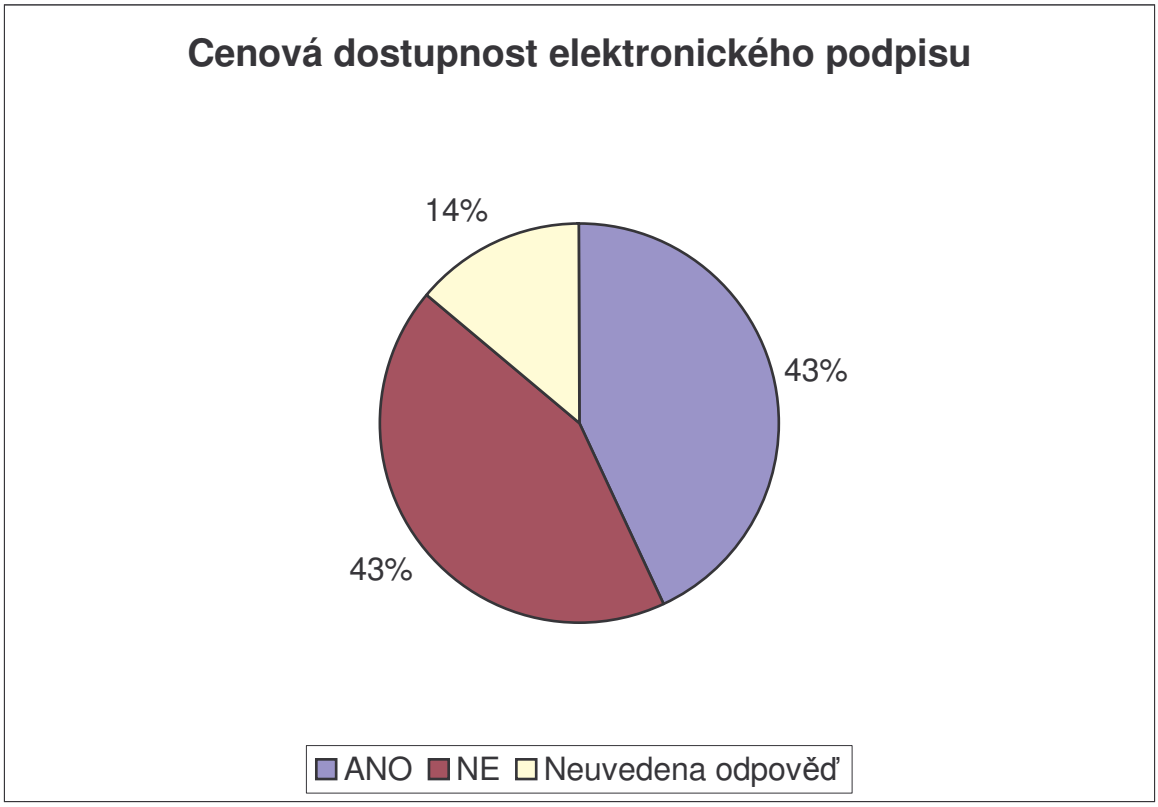
Důkladnější komentář uvádím u následujícího grafu.

Dotaz č. 7: **Myslíte si, že je cena elektronického podpisu pro veřejnost vysoká?**

Zjištěné hodnoty jsou uvedeny v tabulce (Tab. 9)

Možná odpověď	%	Počet
ANO	43	30
NE	43	30
Neuvedena odpověď	14	10

Tab. 9. Cenová dostupnost elektronického podpisu



Graf 9. Cenová dostupnost elektronického podpisu

Ze zjištěných odpovědí usuzuji, že u veřejnosti převládá názor, že pořízení elektronického podpisu je stále drahou záležitostí. Pokusím se na malém příkladu porovnat vzniklé náklady, v případě elektronického podání a podání prostřednictvím pošty. Poplatník, který by chtěl podávat svá daňová přiznání elektronicky si musí asi za 800 Kč zakoupit kvalifikovaný certifikát, s jehož použitím by následně před odesláním svá přiznání elektronicky podepisoval. Využije jej ale jen jednou na konci března, případně ještě několikrát při podání přiznání k silniční dani a DPH. Pokud by poplatník použil kvalifikovaný certifikát

pouze pro podpis přiznání daně z příjmy, tak by jej tento úkon vyšel na 800 Kč, pokud by ještě podával každý měsíc přiznání k DPH a jednou za rok k silniční dani, tak to činí za rok celkem 14 přiznání, cena za jedno podání pak vyjde na 57 Kč.

Pokud ten samý občan místo koupě certifikátu vloží daňové přiznání do obálky a pošle je na finanční úřad, tak jej doporučený dopis a obálka dohromady vyjdou na maximálně 25 Kč. V případě osob samostatně výdělečně činných je situace v případě daně z příjmu ještě komplikovanější. Tito poplatníci musí zajít na FÚ respektive odevzdat přiznání na poště, především proto, že jim správce daně musí pro účely přehledu pro zdravotní pojišťovnu potvrdit, že přiznání odevzdali. Takže pokud by živnostníci přeci jenom chtěli podávat daňová přiznání elektronicky, tak stejně ještě musí zajít na FÚ s formulářem pro pojišťovnu. Domnívám se, že je tohle právě jedna z drobností, které rozvoj elektronického podávání přiznání zbytečně brzdí.

Dotaz č. 8: **Vzděláváte se, či absolvujete pravidelně školení v oblasti elektronického podání daňového přiznání?**

Zjištěné hodnoty jsou uvedeny v tabulce (Tab. 10)

Možná odpověď	%	Počet
ANO	7	5
NE	93	65

Tab. 10. Pravidelné vzdělávání se v oblasti elektronického podání DAP

Graf 8. Pravidelné vzdělávání se v oblasti elektronického podání DAP

Z toho zjištění vyplývá, že veřejnost nemá zájem se pravidelně v této oblasti vzdělávat. V případě potřeby nebo zájmu je možné nalézt všechny potřebné informace, novinky, návody na internetových stránkách Ministerstva financí, které jsou zřejmě pro běžné uživatele elektronického podpisu dostačující.

9 ZHODNOCENÍ VÝVOJE ELEKTRONICKÉ KOMUNIKACE S DAŇOVOU SPRÁVOU

V roce 1999 bylo využito výjimky v legislativě, která umožňovala podávat silniční daň na disketách ve speciální textovém formátu. Určitě to byl jistý pokrok, nicméně značnou nevýhodou byla skutečnost, že podání na nosiči dat nemělo právní účinnost, bylo tedy nutné dodat tzv. zkrácené listinné podání. Přesto byla ještě v tom roce zprovozněna internetová verze podávání daňového přiznání. Ta umožňovala on-line i off-line vyplňování. Tento princip je zachován dodnes.

Dalším zlomovým okamžikem je rok 2001. Od tohoto roku je možno učinit další elektronické podání, a to konkrétně daně z nemovitostí (DNE). V souvislosti se zobecňováním aplikace byl nově vytvořen speciální formát dokumentů – speciální jazyk pro popis datových struktur, který je možno upravit „na míru" poplatníka. Tzn., že umožňuje podávat strukturované dokumenty a při vyplňování vést poplatníka nápovědami.

V roce 2002 bylo již umožněno podání přímo po internetu, nicméně stále bez zaručeného elektronického podpisu. K elektronickému podání přibyla další daň – daň z přidané hodnoty (DPH), dodatečné přiznání daně silniční, oznámení o nezdaněných příjmech (tzv. hlášenky).

Průlomovým je rok 2003, kdy počínaje únorem je možné plné elektronické podání, a to díky zavedení elektronického podpisu („ZAREP"). Jedná se ovšem převážně o daňová přiznání podaná daňovými poradci.

Daňová přiznání za rok 2005 by se mohla masivně podávat prostřednictvím internetu, tedy pokud by byl ze strany vedení MF ČR skutečný zájem. Důležité je zbavit se přemrštěných požadavků na bezpečnost. Je třeba vytvořit takové řešení, které bude klást jen minimální nároky na daňové poplatníky a současně bude přiměřeně bezpečné.

Skutečnost je opravdu taková, že počet daňových přiznání každým rokem roste. Zpracování elektronických podání daňových přiznání MF zahájilo v roce 2002. V roce zveřejnění aplikace bylo uskutečněno pouze 311 podání. V roce 2003 bylo elektronicky podáno 7 018 přiznání k dani. Celkový počet elektronicky uskutečněných podání ke dni 22.3.2006 byl 100 182. Z toho je největší počet 61 222 podání daňových přiznání k DPH. [6].

Pro srovnání předkládám tabulku (Tab. 11), ve které je uvedeno, kolik bylo na Finančním úřadě v Bystřici pod Hostýnem, ze kterého jsem čerpala potřebné informace a údaje

k diplomové práci a využívala metodických materiálů sloužících pracovníkům, podáno daňových přiznání elektronicky za poslední dvě zdaňovací období.

Rok	**2004**		**2005 (stav k 31.3.2006)**	
Daně	**Se ZAREP**	**Bez ZAREP**	**Se ZAREP**	**Bez ZAREP**
DNE	0	1	2	0
DPH	0	0	1	3
DSL	1	1	0	1
DPPO	0	0	0	0
DPFO	2	0	0	0
Hlášenky	0	0	0	0
Celkem	**3**	**2**	**3**	**4**

Tab. 11. Počet elektronického podání přes internet v ADISu

Realizace možnosti elektronického podání daňového přiznání se zaručeným elektronickým podpisem je stále na svém počátku a výše uvedená tabulka je důkazem toho, že poplatníci, tedy alespoň v oblasti působnosti sledovaného úřadu, uvedený způsob podání příliš nevyužívají. Domnívám se, že většina ani neví, že je možné učinit podání tímto způsobem, a nebo nemá k dispozici potřebné technické zařízení s připojením do sítě Internet. Tuto možnost podání tedy, i dle zjištění z dotazníků, využívají především velké organizace nebo daňoví poradci a účetní. Pro poplatníky, kteří komunikují s finančním úřadem pouze jednou za rok, není tato možnost až tak výhodná, dá se říci, že i příliš drahá, protože certifikační autority si za poskytnutí certifikátu účtují poplatky, které se mohou mnohdy zdát vysoké.

Uplatnění elektronického podpisu v praxi dnes v České republice velmi vázne. Paradoxně i proto, že tvůrci nových aplikací by chtěli bezpečnost a identifikaci osob řešit téměř výhradně prostřednictvím elektronického podpisu a současně chtějí hned od počátku vydělávat na provozování certifikačních autorit a dalších službách spojených s elektronickým

podpisem. Výsledkem jsou zmatky, malé rozšíření elektronického podpisu a ztrátovost provozu certifikačních autorit. Jedním z důvodů může být i malá respektive špatným směrem vedená komunikace mezi tvůrci nových aplikací a vlastníky, případně zadavateli nové aplikace. Domnívám se, že v naprosté většině případů mají informatici a uživatelé jiné představy a obtížně hledají společnou řeč.

10 SHRNUTÍ A DOPORUČENÍ

Díky schválení zákona 227/2000 Sb., o elektronickém podpisu a novele zákona 337/1992 Sb., o správě daní a poplatků je umožněno daňovým subjektům a dalším osobám činit podání adresovaná správcům daně prostřednictvím datové zprávy opatřené zaručeným elektronickým podpisem. V případě, že takovým podáním je daňové přiznání, hlášení nebo vyúčtování, musí ho daňový subjekt podat ve struktuře a tvaru zveřejněném správcem daně. U těchto specifických podání zůstává tedy daňový subjekt nadále závislý na orgánech daňové správy. Nyní je možno elektronickým způsobem podat daňové přiznání k dani z přidané hodnoty, k dani silniční, k dani z nemovitosti a k dani z příjmu. Dle zjištění, ale můžu uvést, že tento způsob podání není zatím mezi poplatníky příliš obvyklý a využívají ho především daňoví poradci.

Zavedení elektronické komunikace je pro finanční úřad a měl by být i pro poplatníka značným přínosem, neboť tento způsob komunikace šetří čas, a při častějším využití, i peníze. Daňový poplatník, který chce splnit svoji daňovou povinnost, se připojí na server Ministerstva financí a stáhne si kód aplikace, která mu umožní vyplnit konkrétní formulář daňového přiznání. Tento způsob podání je pro poplatníky snažší, jelikož jsou při vyplňování vedeni nápomocnou aplikací. U ručního vypisování daňového přiznání má poplatník samozřejmě také nápovědu - „pokyny k vyplnění přiznání“, které však mohou být pro některé mnohdy nesrozumitelné a zbytečně obsáhlé. Díky složitosti daňového přiznání se stále častěji stává, že poplatníci finančnímu úřadu odevzdají daňové přiznání s chybami, které musí správce následně pomocí další písemné dokumentace odstranit, čímž se tedy doba vyměření daně zbytečně prodlužuje a tím i prodražuje. Je proto logické umožnit občanům a organizacím využít potenciál výpočetní techniky pro přímou elektronickou komunikaci s finančním úřadem, usnadnit jim mnohdy značně obtížné ruční vyplňování daňových podání a v neposlední řadě uvolnit kapacitu pracovníků daňové správy směrem od ručního pořizování dat z listinných dokumentů k automatizovanému daňovému řízení s použitím zkontrolovaných a autorizovaných elektronických dat.

Jedním z nejdůležitějších úkolů při zavádění elektronického podpisu do praxe bylo vyložit zákonné pojmy, které byly dosud aplikovány pouze na listinné dokumenty, v novém kontextu elektronických písemnostech. Jedná se zejména o pojmy důležité pro daňového poplatníka, jako podání a datum jeho účinnosti, vydání potvrzení pro poplatníka, doručování rozhodnutí poplatníkovi, nahlížení do spisu (který může být elektronický) atd. Toto všech-

no jsou pojmy, které jsou podstatné při jakémkoli sporu mezi poplatníkem a daňovou správou, v případném soudním sporu a mají své důsledky v boji proti daňovým únikům.

Metodická podpora zavedení elektronického podpisu do praxe FÚ by měla být spojena s vydáním uceleného souboru nových řad metodických pokynů, školením pracovníků správy, informační kampaně apod. Všechny dosavadní systémy vycházely z listinného dokladu s vlastnoručním podpisem, který byl pokládán za jediný průkazný doklad, a případná elektronická podoba dokumentů sloužila pouze k usnadnění práce s údaji z dokumentů, k rychlé operativní výměně pracovních verzí dokumentů, případně k výměně údajů mezi úřady státní správy, pokud se ovšem na tom obě strany shodly. Tento stávající systém založen na klasickém podepsaném, případně orazítkovaném dokladu v listinné podobě, bude postupně nahrazen novým systémem.

Nový systém s elektronickým podpisem vychází z toho, že některé dokumenty můžou existovat jen v elektronické podobě. To ale také znamená, že nový systém nelze zavést osamoceně v rámci jednoho úřadu státní správy (tedy např. jen v rámci finančních úřadů), ale v širším rozsahu. Minimálně však na tuto skutečnost musí být připraveny soudy a další instituce, které například vyžadují potvrzenou kopii daňového přiznání, a to jak po organizační, tak technické stránce. Práce s elektronickými dokumenty, zejména pak dokumenty opatřenými elektronickým podpisem, budou vyžadovat technické zabezpečení na výrazně vyšší úrovni než u běžných systémů. Musí zaručovat bezpečné uložení a ochranu všech dokumentů, aby nemohlo dojít k jejich úmyslnému či neúmyslnému poškození, umožňovat trvalý přístup všech oprávněných pracovníků. Má rovněž vyšší nároky na prokazování totožnosti všech uživatelů systému. Vzhledem k náročnosti takovýchto systémů je třeba je realizovat pokud možno jako centralizované, což v řadě případů opět může vést k organizačním změnám v rámci úřadů.

10.1 Další vývoj

Dalším krokem, který by měl zefektivnit daňové řízení je možnost elektronického podání tzv. obecné písemnosti, libovolného podání s textem poplatníka, v požadované struktuře. Nešlo by tedy o podání formuláře, ale například určitého dopisu. Tento obecný formát písemnosti byl měl umožnit nabalit na prostý text obálku s příslušnými razítky, respektive potvrzeními. Komunikace s úřadem je pak možná stejným způsobem jako u daňového formuláře.

Dle mého názoru využití prostředků e-governmentu podstatným způsobem zefektivní jak plnění daňových povinností občana či organizace, tak zpracování daňových podání na straně daňové správy, které je v současné době téměř u všech daní na pracovišti realizováno, bohužel ze strany poplatníků ale stále minimálně využíváno.

ZÁVĚR

Se vstupem do 21. století je více než kdy jasné, že prosperující společnost musí zvládnout nejmodernější technologie, zapojit se do elektronického obchodu, zajistit bezpečnou a důvěrnou komunikaci mezi jednotlivými občany, zajistit ochranu osobních dat, zajistit vyřizování požadavků občanů na státní správu, zavést elektronické peníze a v neposlední řadě zajistit uznání elektronického podpisu, jako jednoho ze základních kamenů elektronické společnosti. Lidé ve společnosti, která nezajistí tyto zcela zásadní úlohy, nemohou počítat s tím, že se zařadí mezi moderní, prosperující národy. Při vytváření prostředí legislativního, ekonomického, vědeckého je potřeba respektovat daný stav v Evropské unii. V případě základních zákonů a právních norem pak jsem přímo povinni slaďovat naše zákony se zákony platnými v Evropské unii.

Zákon o elektronickém podpisu je naprosto nezbytným základem k budování moderní společnosti, v pravém slova smyslu nám může otevřít dveře do velkého obchodu 21. století. Je důležitým krokem na cestě ke zrovnoprávnění vlastnoručního a digitálního podpisu. Tento důsledek skýtá široké možnosti uplatnění nových technologií a jejich rozvoje. Běžným uživatelům dává možnost bezpečné komunikace na všech úrovních, a to vše v čase nesrovnatelně rychlejším, než bylo zvykem. Právní úprava elektronického podpisu je zcela nutnou a bezpodmínečnou kapitolou vstupu České republiky do společnosti západních států.

Při zpracování dané problematiky jsem se snažila hledat objektivní kvality a nedostatky současné situace elektronického podpisu v praxi a věřím, že tato práce bude alespoň minimálním přínosem k pochopení a řešení problematiky elektronické komunikaci s daňovou a částečně veřejnou správou.

SEZNAM POUŽITÉ LITERATURY

Monografické publikace:

[1] BOSÁKOVÁ, D., aj. *Elektronický podpis*. 1. vyd. Olomouc: ANAG, 2002. ISBN 80-7263-125-X

[2] DOBDA, L. *Ochrana dat v informačních systémech*. 1. vyd. Praha: Grada Publishing, 1999. ISBN 80-7169-479-7

[3] JAŠEK, R. *Ochrana znalostí a dat v podnikových informačních systémech.* 1.vyd. Zlín: UTB Zlín 2002. ISBN 80-7318-095-2

[4] RYBKA, M. *Jak komunikovat elektronicky*. 1. vyd. Praha: Grada Publishing, 2002. ISBN 80-247-0208-8

Časopisy:

[5] E-government č. 3/2003

Internetové stránky:

[6] http://www.mfcr.cz

[7] http:// www.mvcr.cz

[8] http://www.uoou.cz

[9] http://www.bis.cz

[10] http:// www.e-podpisy.cz

[11] http://www.egovernment.cz

Použité právní předpisy:

[12] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů

[13] Vyhláška Úřadu pro ochranu osobních údajů č. 366/2001 Sb., o upřesnění podmínek stanovených v § 6 a 17 zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů

[14] Směrnice 1999/93/Es, o zásadách Společenství pro elektronické podpisy

[15] Pokyn č. D–252 – podmínky pro podání v daňových věcech prostřednictvím datové zprávy (podání v elektronické podobě)

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ZoEP Zákon č. 227/2000 Sb., o elektronickém podpisu

EU Evropská unie

IT Informační technologie

FÚ Finanční úřad

ADIS Automatizovaný daňový informační systém

FŘ Finanční ředitelství

ÚFDŘ Ústřední finanční a daňové ředitelství

EPO Elektronická podání

ZAREP Zaručený elektronický podpis

DNE Daň z nemovitosti

DPH Daň z přidané hodnoty

DPFO Daň z příjmu fyzických osob

DPPO Daň z příjmu právnických osob

DSL Daň silniční

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH