VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE
FAKULTA FINANCÍ A ÚČETNICTVÍ
katedra finančního účetnictví a auditingu

hlavní specializace: **Účetnictví a finanční řízení podniku**

Bc. Ladislav Guzý

Elektronický podpis a jeho využití v účetnictví

Vedoucí diplomové práce: doc. Ing. Ladislav Mejzlík, Ph.D.

2014

Čestné prohlášení:

Prohlašuji, že jsem tuto diplomovou práci zpracoval samostatně a veškerá použitá literatura a další prameny jsou řádně označeny a uvedeny v přiloženém seznamu.

V Praze dne

…….....

Podpis

Poděkování

Touto cestou bych rád poděkoval panu doc. Ing. Ladislavu Mejzlíkovi, Ph.D. za odborné vedení, cenné rady, náměty a předané zkušenosti, které mi velice pomohly při vypracování této diplomové práce.

Dále bych chtěl poděkovat všem respondentům, kteří se zúčastnili dotazníkového šetření k této práci, za jejich ochotu a čas. Nakonec bych chtěl také poděkovat své rodině za podporu po celou dobu mého studia.

Abstrakt:

Diplomová práce se zabývá problematikou elektronického podpisu a jeho využití v účetnictví a podnikatelské činnosti obecně. Práce je strukturována do dvou částí, z nichž první zahrnuje obecný rozbor pojmů a charakteristických znaků elektronického podpisu, certifikátů a certifikačních autorit a časových razítek, včetně analýzy silných a slabých stránek využívání těchto služeb. V závěru této teorie jsou nastíněny některé nejčastější možnosti využití elektronického podpisu v účetním systému firem. Na tuto část navazuje rozbor samotného praktického využívání elektronického podpisu v současné době, provedený průzkumem v rámci podnikatelské sféry prostřednictvím dotazníkového šetření a analýzou výsledků.

Klíčová slova:

Elektronický podpis, archivace elektronických dokumentů, časové razítko, certifikát, certifikační autorita, hashovací funkce, historický vývoj elektronického podpisu

Abstract:

Diploma thesis is focused on matters of electronic signatures and their possible usage in accounting and business process. The paper is divided into two parts. Subject of the first part is general analysis of terminology and characteristics of electronic signature, certificates and certification authorities and time stamps, including analysis of strengths and weaknesses of these services. At the end of this theory part are outlined some of the most common choices of using electronic signature in accounting system. In second part are analysed results of research, which was performed by sending questionnaire to a number of randomly chosen companies.

Key words:

Electronic signature, digital signature, archiving of electronic documents, time stamp, certificate, certification authorities, hash, hash algorithm, historical development of electronic signature

Obsah

ÚVOD 1

1 HISTORICKÝ VÝVOJ 3

1.1 Počátky kryptografie 3

1.2 Elektronický podpis ve světě 4

1.3 Elektronický podpis v České republice 5

2 ELEKTRONICKÝ PODPIS 8

2.1 Podstata elektronického podpisu 9

2.2 Hashovací funkce 10

2.3 Zaručený elektronický podpis 14

2.4 Certifikát a certifikační autority 14

2.4.1 Certifikát 15

2.4.1.1 Certifikáty poskytovatelů certifikačních služeb 17

2.4.1.2 Klientské certifikáty 18

2.4.2 Certifikační autorita 19

2.5 Časová razítka 22

3 SILNÉ A SLABÉ STRÁNKY ELEKTRONICKÉHO PODPISU 24

3.1 Výhody elektronického podpisu 24

3.2 Nevýhody elektronického podpisu 25

4 LEGISLATIVNÍ ÚPRAVA 28

4.1 Evropská unie 28

4.2 Česká republika 29

4.3 Slabé stránky současné právní úpravy v České republice 30

5 VYUŽITÍ ELEKTRONICKÉHO PODPISU V ÚČETNICTVÍ 33

5.1 Elektronická fakturace 33

5.2 Interní využití 34

5.3 Komunikace s orgány státní správy a samosprávy 38

5.3.1 Datové schránky 39

5.3.2 E-podatelny a Daňový portál 40

5.4 Archivace účetních dokladů 41

6 PRAKTICKÁ ČÁST 46

6.1 Proces dotazníkového šetření 46

6.2 Struktura respondentů dle základních charakteristik 47

6.3 Analýza výsledků 49
6.3.1 Společnosti nevyužívající elektronický podpis 50
6.3.2 Společnosti využívající elektronický podpis 54
6.3.3 Shrnutí kladů a záporů dle respondentů 63
ZÁVĚR 67
ZDROJE 72
Odborná literatura 72
Zdroje pro praktickou část 72
Právní předpisy 73
Ostatní zdroje 74
PŘÍLOHY 77
Seznam obrázků 77
Seznam tabulek 77
Seznam grafů 78
Dotazník 79

Úvod

Historie lidstva je protkána problémem jednoznačné identifikace osob. Každého člověka můžeme identifikovat různými způsoby. Od typických znaků viditelných pouhým okem jako například barva či délka vlasů, velikost nebo tvar očí, výška a jiné tělesné dispozice apod., přes jejich DNA a otisky prstů až po jejich jméno. S vynálezem písma a jeho pozdějším rozšířením, však vyvstala potřeba nějakým snadným způsobem tuto identitu dané osoby zachytit. Východiskem se stal vlastnoruční podpis. Ten hrál po velkou část historie nezastupitelnou úlohu, a přestože i v dnešní době má velkou váhu, s relativně nedávným rozmachem výpočetních technologií, a to především internetu, bylo nutné vyvinout způsob, jak se identifikovat také v tomto digitálním světě. Zmíněný problém vyřešil elektronický podpis, o kterém pojednává tato diplomová práce.

Toto téma jsem si zvolil, jelikož se domnívám, že elektronický podpis může zajistit průkazné předávání a automatické zpracovávání veškeré nejen externí, ale také interní komunikace firem. A to do takového stádia jeho využívání, kdy ho budou používat nejen podniky, ale také soukromé osoby při běžné komunikaci například prostřednictvím emailu. I v dnešní době však elektronický podpis využívají spíše společnosti, kterým to ukládá zákon nebo významný odběratel či dodavatel s dostatečnou ekonomickou silou a prostředky pro jeho prosazení. Je to způsobeno hlavně nedostatky v legislativní úpravě a nedostatečnou informovaností soukromých osob.

Cílem této práce je posoudit praktické využití a provést průzkum používání elektronického podpisu v účetnictví podnikatelů, obchodních společností a orgánů státní správy a samosprávy. Dále také implementace jednotlivých prvků do legislativy České republiky.

Diplomová práce je rozdělena do dvou ucelených částí. V první polovině je rozebrána teoretická stránka této problematiky. Charakteristika elektronického podpisu, časových razítek a certifikačních autorit a jejich legislativní úprava. Následuje pak samotné využití elektronického podpisu v účetnictví.

Druhým celkem je praktická část, v rámci které byl rozeslán dotazník podnikatelům a firmám o různé velikosti, formě i oboru podnikání. Nachází se zde grafické zobrazení a analýza získaných odpovědí.

1 Historický vývoj

V průběhu vývoje elektronické komunikace vznikaly různé nároky především na její zabezpečení. Na počátku se jednalo pouze o komunikaci prostřednictvím emailu a tedy jednoduchou záměnu papírových písemností jejich elektronickými ekvivalenty. Ve druhé fázi se objevovaly první „základní, jednoduché, pasivní webové stránky v podstatě zahrnující elementární informace o konkrétní firmě“.[1] Tyto stránky se posléze doplnily o další údaje, jako je sortiment vyráběných produktů firmy či jejich služeb. Do této chvíle zabezpečení nebylo prioritou z důvodu pasivity poskytovaných informací touto elektronickou cestou.

Zlomovým bodem se stalo rozšíření obchodování prostřednictvím internetu. Aby mohlo fungovat, bylo nutné identifikovat zákazníka za účelem vymáhání platby za poskytnuté zboží či služby. V dnešní době již tento prvek není ničím novým a každý větší podnik nabízí svým zákazníkům uzavření, vypořádání a dokonce i sledování své objednávky elektronicky prostřednictvím internetu. Pokud je tedy veškerý kontakt subjektů na elektronické úrovni, pak je nutné najít i ekvivalent vlastnoručního podpisu zajišťující stejné funkce. Těmi je již zmíněná identifikace autora podpisu, dále snadné zjištění případných pozdějších změn v dokumentu a v neposlední řadě musí tato náhrada také představovat neodvolatelný právní úkon. Veškeré tyto podmínky spolu s některými dalšími výhodami zajišťuje elektronický podpis.

1.1 Počátky kryptografie

Elektronický podpis jako takový je možné označit za určitý způsob šifrování dat. Prvopočátky šifrování se objevují již 4500 před. n. l. ve starověkém Egyptě. Více méně je možné historicky spojit potřebu utajení informací již s prvními známkami písma. V dnešní době je však naprostá většina dat v elektronické podobě a výpočetní výkon roste takovým tempem, které vyžaduje neustálé zdokonalování metod kódování. Jako první se objevila symetrická kryptografie, která využívala jednoho „klíče“ (hesla, šifrovacího algoritmu). Problémem však bylo předání tohoto klíče od jednoho subjektu k druhému bez jeho úniku třetí straně. Na základě této potřeby vznikla v roce 1970 asymetrická kryptografie vyvinutá Jamesem Ellisem z britské CESG (Communications – Electronics Security Group). Její konkrétní obdoba RSA (zkratka z prvních písmen

[1] Budiš, P. - Elektronický podpis a jeho aplikace v praxi, 2008, str. 10

tvůrců systému Rivest, Shamir a Adelmann z roku 1978) byla vyvinuta, jak se později ukázalo, již v roce 1973 Cliffordem Cocksem taktéž z instituce CESG.[2] Zmíněný systém je mimo jiné dodnes nejznámějším a nejpoužívanějším jádrem elektronických podpisů. Podrobněji je asymetrická kryptografie rozebrána v kapitole *Elektronický podpis*.

1.2 Elektronický podpis ve světě

Základy celosvětového veřejného využívání elektronického podpisu položily Spojené státy americké prostřednictvím tří zákonů. Konkrétně se jednalo o California Digital Signature Regulations (1998) a na ně navazující UETA (Uniform Electronic Transactions Act, 2000) a ESIGN (Electronic Signatures in Global and National commerce Act, 2001). Společně tyto právní předpisy definují podmínky a pravidla zavedení elektronického podpisu na státní, federální a globální úrovni.[3]

Evropská unie následně vydala vlastní předpis, který vychází z americké legislativy, a to směrnici 1999/93/EC, ze dne 13. prosince 1999, o zásadách Společenství pro elektronické podpisy. Jejím účelem bylo ustanovení všeobecných pravidel pro používání elektronických podpisů v rámci unie jako opatření proti „rozdílům v předpisech členských států o právním uznání elektronických podpisů a o akreditaci ověřovatelů“[4], a tím také posílení důvěry v nové technologie a jejich obecné uznání.

Počátek využívání šifrování obecně a elektronického podpisu širokou veřejností samozřejmě kladl vyšší nároky na jeho bezpečnost. Pod záštitou IST Programu Evropské komise dne 1. ledna 2000 odstartoval tříletý projekt NESSIE (New European Schemes for Signature, Integrity, and Encryption), který měl za úkol vyvinout algoritmy s vyšším zabezpečením a důvěryhodností. V jeho obsahu se mimo jiné nacházelo i vylepšení hashovacích funkcí a digitálních podpisů.

Poté, dne 16. října 2009, Komise Evropského společenství vydala rozhodnutí (platné od 28. prosince 2009)[5], které „ukládá členským státům povinnost uvést do provozu nástroj umožňující vzájemné uznávání kvalifikovaných certifikátů,

[2] Vondruška, P. - CoputerWorld 37/2000-40/2000
[3] Lewis, D. Levey - B2C Electronic Signatures: Building Stronger Consumer Relationships
[4] Oficiální překlad směrnice 1999/93/EC; http://isap.vlada.cz/
[5] Rozhodnutí Komise 2009/767/ES

na kterých jsou založeny zaručené elektronické podpisy.“[6] Jedná se o tzv. TSL (Trusted Services Lists) seznamy všech akreditovaných certifikačních autorit. Rozhodnutí ale nebylo bez určitých nesrovnalostí konkrétně v rovině formátů elektronických podpisů, které se vyřešily až jejich sjednocením v rozhodnutí Komise účinným od 1. srpna 2011.[7]

1.3 Elektronický podpis v České republice

V České republice bylo teoreticky možné vést účetnictví prostřednictvím výpočetní a jiné techniky od 1. ledna 1992, kdy vešel v platnost zákon č. 563/1991 Sb., o účetnictví, avšak s jeho praktickou aplikací vyvstávaly mnohé problémy. Jedním z nich byla i potřeba účetního dokladu jako originální písemnosti.[8] Ty byly samozřejmě spojené s podpisy různých odpovědných osob, které v tuto dobu měly pouze písemnou formu. Technické prostředky elektronického podpisu, jak je zmíněno výše, již však existovaly. Překážkou bránící jejich používání byla neexistence její právní regulace, jinými slovy zrovnoprávnění elektronického a vlastnoručního podpisu.

V roce 2000 měl tedy Úřad pro státní informační systém za úkol sestavit první návrh zákona o elektronickém podpisu. Nicméně z důvodu dlouhé doby přípravy se iniciativy nakonec chopilo sdružení SPIS (Sdružení pro informační společnost, jejím následovníkem je dnes ICT unie). První verze zákona byla prezentována 23. září 1999. Autorem byl doc. Vladimír Smejkal a spoluautorem doc. Pavel Mates. K této podobě však měla odborná veřejnost určité připomínky, které byly zpracovány a aktualizovaný návrh, publikovaný pod stejným autorem, byl předložen parlamentu 26. ledna 2000, kde prošel 1. čtením. V čase do 2. čtení byla mezitím vydána direktiva Evropské unie 1999/93/EC zmíněná v předchozí podkapitole, která podnítila obě instituce po vzájemné dohodě k ustanovení skupiny odborníků s cílem zapracovat tuto směrnici do připravovaného zákona. Výsledkem této snahy byl značně upravený koncept doručený předkladatelům zákona 7. března 2000. „Oproti původním dohodám a slibům však byla tato verze ještě dále měněna, mj. i autorem předchozích verzí doc. Smejkalem, a znovu do ní byly zaneseny některé dřívější omyly a chyby.“[9] Tyto modifikace vedly až k veřejnému distancování se členů odborné skupiny od výsledného

[6] Ministerstvo vnitra ČR, Odbor koncepce a koordinace ICT ve veřejné správě, 27. 6. 2011
[7] Rozhodnutí Komise 2011/130/EU
[8] Mejzlík, L. - Účetní informační systémy: využití informačních a komunikačních technologií v účetnictví, 2006, str. 58
[9] Peterka, J. - Česká cesta k elektronickému podpisu?, IT-NET, 2000

znění. Finální podobu návrhu zákona dne 11. července 2000 podepsal prezident České republiky a dne 1. října 2000 vešel v platnost zákon č. 227/2000 Sb., o elektronickém podpisu. Tento nový právní předpis byl především důležitý pro začátek nové éry vedení účetnictví na počítači. Aby však bylo možné toho využít v plném rozsahu a bez překážek, dalším nezbytným krokem byla novela zákona o účetnictví č. 353/2001 zrovnoprávňující různé formy účetního záznamu a platná od 1. ledna 2002.

I přes značnou snahu vlády, měl zákon o elektronickém podpisu mnoho nesrovnalostí a aplikovatelný na praxi byl v podstatě až po jeho relativně zásadní novele č. 440/2004 Sb., která upravovala především:

- „časová razítka,
- vydávání kvalifikovaných systémových certifikátů pro potřeby tvorby elektronických značek,
- používání bezvýznamového identifikátoru osob MPSV,
- možnost udělení akreditace poskytovateli certifikačních služeb, který je organizací veřejné správy.“[10]

Následujícími mezníkem v historickém vývoji z hlediska podepisování elektronických dat byl rok 2006, kdy vešla v platnost vyhláška č. 378/2006 Sb., týkající se mimo jiné:

- postupů kvalifikovaných certifikačních autorit,
- požadavků na nástroje elektronického podpisu,
- ochrany dat pro vytváření elektronických značek.

Velký důraz je zde kladen na první zmíněný bod a zabezpečení poskytovatelů certifikačních služeb.

Posledním právním předpisem významně modifikujícím zákon o elektronickém podpisu je zákon č. 167/2012 Sb., v platnosti od 1. července 2012. Kromě změny některých definic základních pojmů obsahuje:

[10] Mejzlík, L. - Účetní informační systémy: využití informačních a komunikačních technologií v účetnictví, 2006, str. 37

- nařízení kvalifikovanému poskytovateli certifikačních služeb předat každý rok ministerstvu (v současné době Ministerstvo vnitra) seznamy zneplatněných certifikátů,
- vymezení *uznávaného elektronického podpisu*,
- povinnost ministerstva umožnit dálkový přístup k informacím o podmínkách ověření uznávaného elektronického podpisu a značky,
- zapracování rozhodnutí Komise 2011/130/ES a 2009/767/ES.[11]

[11] Zákon č. 227/2000 Sb., o elektronickém podpisu ve znění pozdějších předpisů

2 Elektronický podpis

Pro bezproblémovou funkčnost musí elektronické komunikace splňovat různé požadavky na bezpečnost. Ty jsou shrnuty v následujících kritériích:

- Dostupnost
- Důvěrnost
- Integrita
- Autentizace a autorizace
- Nepopiratelnost
- Přesný čas transakce

Předpokladem pro využití různých systémů samozřejmě je, aby byly za účelem bezproblémové komunikace co nejlépe dostupné. Velice často se navíc jedná o výměnu citlivých informací a je tedy nutné zabezpečit takový přenos, jenž znemožní jejich čitelnost neoprávněnou třetí stranou a zaručí snadnou identifikaci jakýchkoli případných změn. Před zahájením samotné výměny dat je nezbytné určit identitu obou komunikujících stran, nejen v daný okamžik ale i následně, a jejich přístupová práva. Na která kritéria je kladen větší důraz, se liší dle subjektů účastnících se této komunikace. Elektronický podpis může řešit mnohé z těchto požadavků. Nicméně je určen pouze pro fyzické osoby. Právnické osoby mají možnost využít ekvivalentní službu, kterou je elektronická značka. Rozdílem je to, že značka neidentifikuje konkrétní osobu, ale společnost, za kterou se může podepisovat více zaměstnanců oprávněných podepisovat dokumenty jménem společnosti, nebo tak může činit automaticky programové vybavení apod.

Cesta k dnešní podobě a využívání elektronického podpisu byla obtížná, jak již naznačuje předchozí kapitola. Některé aspekty přesto nejsou dodnes vyřešené. Největším problémem v dnešní době je vysoká míra neinformovanosti veřejnosti o základních pojmech a výhodách jeho používání. I přes masivní rozšíření internetové komunikace a moderních technologií si naprostá většina lidí pod pojmem „podpis“ představí ten vlastnoruční. Dle jejich mínění by tento podpis bylo možné převést na elektronický podpis pouhým „naskenováním“. S touto chybou se lze doposud setkat téměř u všech soukromých osob. Stále je však možné, i přes jejich naprosto odlišnou podobu, najít analogii mezi oběma formami. Oba například plní stejné funkce a mají

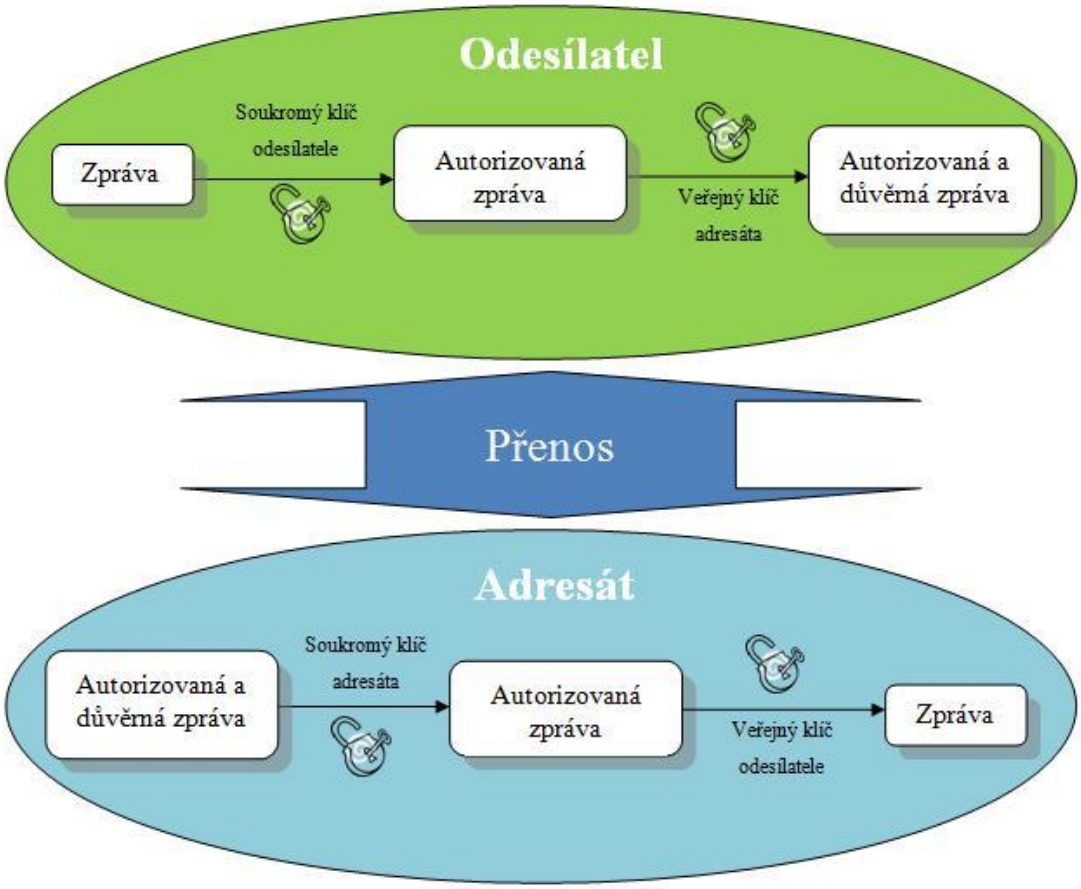
dva různé stupně míry jistoty s nimi spojené. Podrobnější porovnání je možné najít v podkapitolách *Výhody elektronického podpisu* a *Nevýhody elektronického podpisu*.

2.1 Podstata elektronického podpisu

Elektronický podpis je založen na tzv. *asymetrické kryptografii*. Tento způsob šifrování je založen na dvou „klíčích“. Princip klíče je možné nejlépe vysvětlit na příkladu procesně jednodušší *symetrické kryptografie*. Tzv. Césarova šifra byla vyvinuta již starověkými Římany, odkud pochází i její název. Používala se pro předávání zpráv mezi legiemi a princip spočíval v zaměnění každého písmena za jiné, umístěné v abecedě o tři místa dále. Znalost této náhrady by se pak dalo považovat za onen klíč. V moderních technologiích existuje jako číslo s velkým množstvím decimálních míst. Avšak v tomto triviálním příkladě je použit pouze jediný pro šifrování i dešifrování zprávy. Asymetrická kryptografie vychází z existence dvou těchto klíčů, jedním se zpráva zakóduje a druhým dekóduje, a naopak. Obvykle si je stanoví sám majitel pomocí všeobecně dostupných matematických algoritmů, kdy jeden z nich je stanoven a druhý odvozen. Za předpokladu, že není možné tento proces provést v opačném směru, označuje se takováto dvojice za *kryptografii s veřejným klíčem* používající se u elektronického podpisu.

Následující schéma znázorňuje nejjednodušší případ použití elektronického podpisu při předání zprávy od odesilatele k adresátovi.

Obrázek 1 Proces podepsání a přenosu datové zprávy



Zdroj: Vlastní zpracování

Tento případ však není v praxi použitelný. Je to způsobeno podstatou asymetrické kryptografie, která je mnohem komplikovanější než symetrická, a klade mnohem větší nároky na výpočetní výkon. Podepisování celé zprávy by při současných možnostech zabralo příliš mnoho času. Z toho důvodu byla vynalezena tzv. *hashovací funkce*.

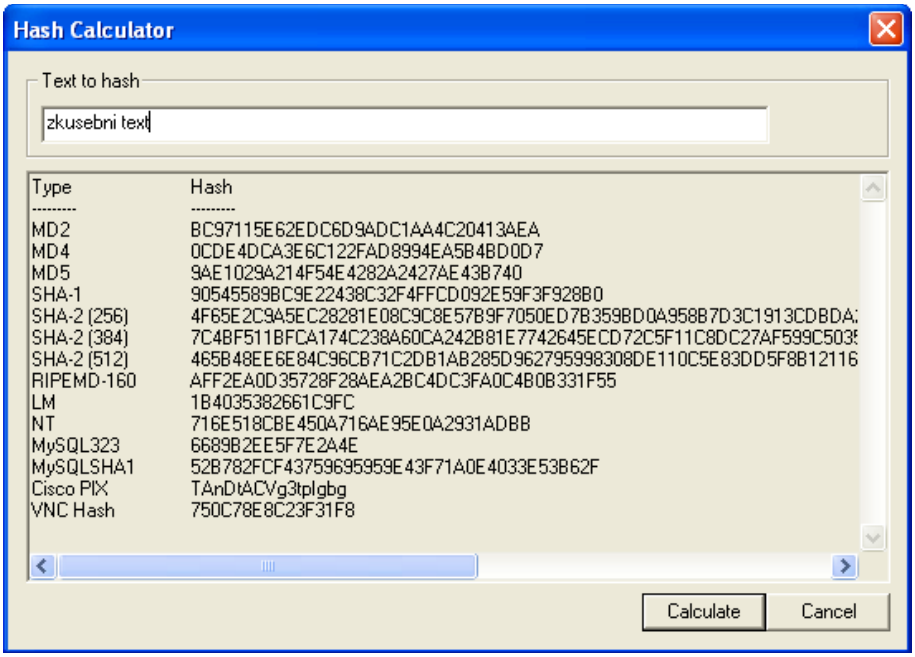
2.2 *Hashovací funkce*

Hashovací funkce vytvoří z každé zprávy nezaměnitelný otisk neboli „hash“ (různé zdroje ho nazývají také jako fingerprint či digitální otisk zprávy), který má vždy stejnou, předem definovanou délku bez ohledu na velikost původní datové zprávy. Nejrozšířenějšími algoritmy pro jejich vytváření jsou MD-5, SHA-1 a SHA-2 zabudované do různých volně dostupných programů. Každý algoritmus je

ale použitelný pouze pro určité časové období, při zachování přiměřené míry bezpečnosti, které upravuje dokument ETSI TS 102 176-1.[12]

Tento získaný otisk je specifický pro každý dokument, jež chce odesílatel podepsat. Změna byť i jediného znaku ve zprávě by znamenala změnu celého hashe. Jedná se o jednosměrnou funkci a získat zpětně celou zprávu je tedy téměř nemožné (za jakých předpokladů toto tvrzení neplatí je rozvedeno v kapitole *Nevýhody elektronického podpisu*). Navíc je nepravděpodobná existence dvou různých dokumentů s identickými otisky. Šance výskytu něčeho takového je podobná jako u odvození soukromého klíče pouze se znalostí veřejného. Níže je možné vidět konkrétní příklad jednoduchého hashovacího programu s ukázkou jednotlivých otisků krátkého textu podle různých funkcí.

Obrázek 2 Příklad otisků jednoduchého textu

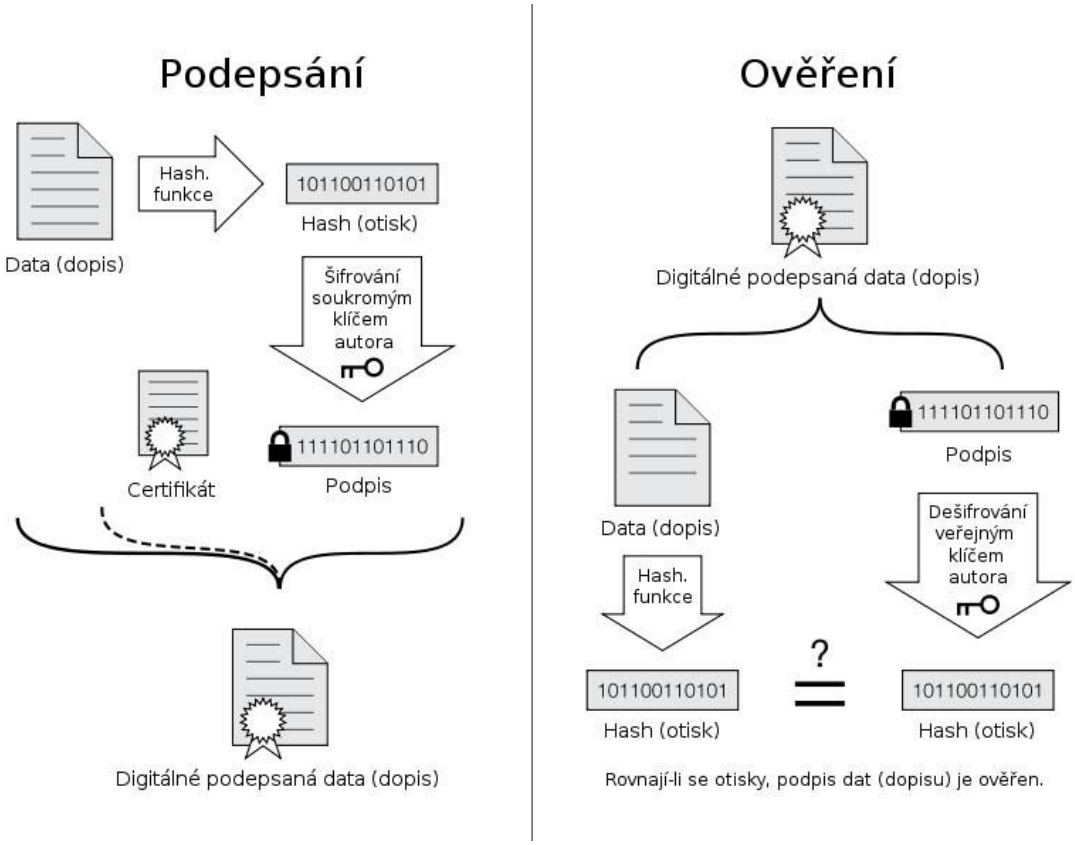


Zdroj: http://www.czechnationalteam.cz/storage/200709071352_4153.png

[12] Budiš, P. - Elektronický podpis a jeho aplikace v praxi, 2008, str. 34

Aby však bylo možné využít elektronického podpisu jako ekvivalentu vlastnoručnímu, je nutné zajistit ověřitelnost jeho vazby na určitou osobu. Pokud by tento požadavek nebyl splněn, mohlo by dojít k situaci, kdy třetí osoba zachytí výměnu veřejných klíčů a nahradí je svými vlastními bez vědomí obou stran. Následující komunikaci přesměruje tak, aby procházela skrze ni. Jako odpověď na tuto hrozbu byly zřízeny certifikační autority (= poskytovatelé certifikačních služeb), které podléhají přísné regulaci a dohledu státu. Tyto společnosti vydávají a evidují takzvané certifikáty, které dokládají identitu vlastníka veřejného klíče (více podrobností o certifikátech a certifikačních autoritách v kapitole jim věnované). Použití těchto modifikací na příkladu je možné vidět na obrázku níže.

Obrázek 3 Proces podepsání a odeslání zprávy a její ověření adresátem



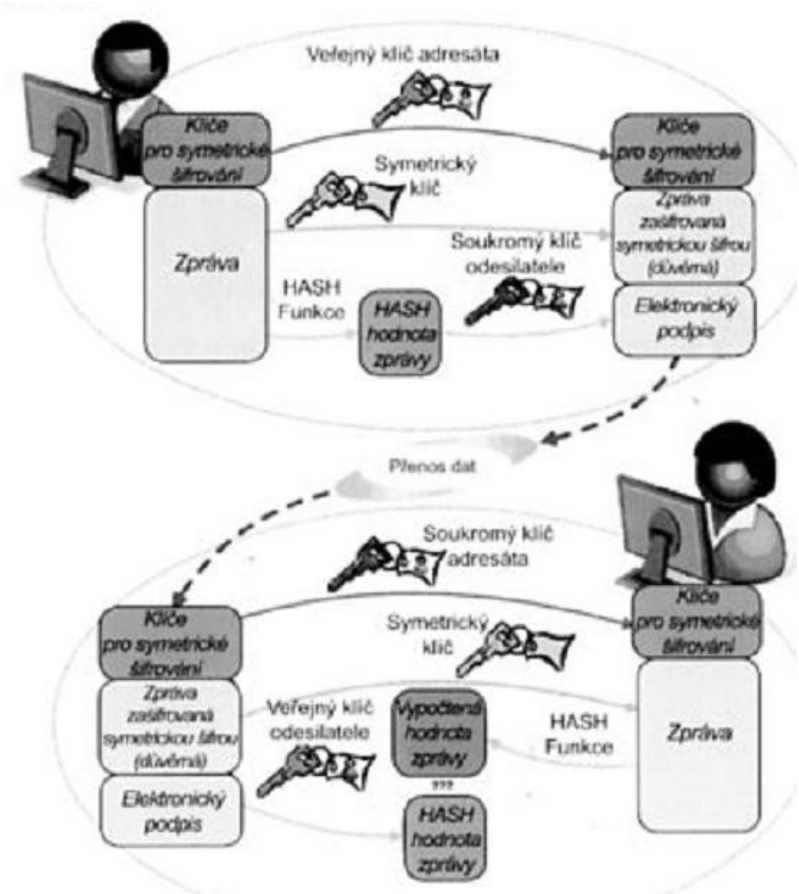
Zdroj: http://www.mirecekp.net/internet/elektronicky-podpis/

Postup je tedy následující. Z původní zprávy odesilatel vytvoří pomocí volně dostupného programu hash. Tento otisk následně zašifruje svým soukromým klíčem, uloženým obvykle na čipové kartě nebo USB flash disku, a tím vznikne elektronický podpis, který může obsahovat i takzvané časové razítko přesně stanovující datum a čas podpisu. Podpis je následně společně s certifikátem a případně i veřejným klíčem

přiložen k původnímu dokumentu a odeslán. Adresát po přijetí dat ověří certifikát u certifikační autority. Poté dekóduje elektronický podpis pomocí obdrženého veřejného klíče, čímž získá otisk zprávy, který porovná s otiskem zprávy vytvořeným hashovacím programem. Jestliže se tyto dva otisky rovnají, získá příjemce jistotu o identitě odesílatele, neporušenosti dokumentu a pokud bylo součástí i časové razítko, pak také o čase podepsání.

Stále ale není vyřešený bezpečný datový tok bez rizika odcizení důvěrných informací třetí stranou. Je nutné spojit obě uvedená schémata do jednoho následovně:

Obrázek 4 Bezpečná komunikace s využitím elektronického podpisu



Zdroj: Budiš, P. - Elektronický podpis a jeho aplikace v praxi, str. 35

V návaznosti na předchozí příklad odesílatel po podepsání datové zprávy a přiložení certifikátu celý tento soubor zašifruje pomocí libovolného symetrického klíče. Ten následně připojí ke zprávě zašifrované veřejným klíčem adresáta. Zabezpečení je tedy na třech stupních s použitím tří různých klíčů. Je tím zaručena nečitelnost zprávy pro kohokoli, kdo nevlastní soukromý klíč určeného příjemce

zprávy. Adresát nejdříve musí dešifrovat symetrický klíč, kterým odemkne dokument s certifikátem. Následně postupuje tak, jak je popsáno v Obrázku 3.

2.3 Zaručený elektronický podpis

Tento specifický typ elektronického podpisu je jeho nadřazenou formou. Vznikl na základě potřeby silnějšího zabezpečení pro jeho využití na stejné právní úrovni jako podpis vlastnoruční. Dosažení tohoto cíle je podmíněno následujícími požadavky. Aby mohl být elektronický podpis označen za zaručený elektronický podpis, musí:

- „být jednoznačně spojen s podepisující osobou,
- umožnit identifikaci podepisující osoby ve vztahu k datové zprávě,
- být vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
- být k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.“[13] [14]

Je tedy zřejmé, že pro vytvoření zaručeného elektronického podpisu v praxi, je nutné využít kryptografických mechanismů pro zajištění identifikace změn v původním dokumentu, a kvalifikovaný certifikát pro zajištění nepopiratelnosti a jednoznačného určení podepsané osoby.

2.4 Certifikát a certifikační autority

Vlastnoruční podpis by sám o sobě neměl vůbec žádný význam, pokud by neměl specifické znaky spojující ho s určitou osobou. Jedná se například o náklon jednotlivých písmen, tlak vyvíjený na propisovací tužku v jednotlivých částech linií, celkový tvar písmen apod. Jednoduché ověření může udělat každý člověk porovnáním s podpisovým vzorem. Jistota pravosti podpisu je však v takovém případě nízká. Pro její zvýšení je již potřeba zkušeného grafologa. I tito odborníci se ovšem mohou dopustit chyby při vyhodnocování umně vyhotoveného falsifikátu.

U elektronického podpisu samozřejmě tato potřeba vyvstává také, a jak již bylo naznačeno v předchozí kapitole, jejím řešením bylo vytvoření certifikátů a nezávislé třetí strany pro jejich správu a dohled nad nimi – certifikačních autorit.

[13] Budiš, P. – Elektronický podpis a jeho aplikace v praxi, 2008, str. 150
[14] § 2 písm. b) zákona č. 227/2000 Sb., o elektronickém podpisu ve znění pozdějších předpisů

2.4.1 Certifikát

Pod tímto pojmem je možné si představit určitá elektronická data ekvivalentní k občanskému průkazu. Jinými slovy se jedná o spojení identity osoby a specifického znaku s ní neoddělitelně spjatého (podpisového vzoru, veřejný klíč elektronického podpisu). Obdobu je možné najít i v časově omezené platnosti, která bývá nejčastěji jeden rok. Rozdílem oproti podpisu vlastnoručnímu, a jeho podpisovému vzoru na občanském průkazu, je míra jistoty o pravosti elektronického podpisu při porovnání certifikátu s veřejným klíčem, která je v tomto případě již maximální. Tento proces probíhá často zcela automaticky a bez nutnosti zásahu další osoby.

Certifikát může existovat v různých formátech, mezi které patří například DER (Distinguished Encoding Rules), PEM (Privacy Enhanced Mail) nebo například i jednoduchý textový formát TXT. Obsah by měl být u jednoho případu však stejný bez ohledu na to, v jakém formátu je prezentován. Podobu konkrétního certifikátu v textové formě je možné vidět níže na výňatku z certifikátu pana Petra Budiše.

Obrázek 5 Výňatek z certifikátu v textovém souboru

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 10142868 (0x9ac494)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CZ, CN=I.CA - Qualified root certificate, O=První
certifikační autorita, a.s.
        Validity
            Not Before: Aug 28 08:56:25 2007 GMT
            Not After : Aug 27 08:56:25 2008 GMT
        Subject: C=CZ, CN=Petr Budiš, O=První certifikační autorita, a.s.,
emailAddress=budis@ica.cz, serialNumber=ICA - 10050831
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:e1:c3:f8:f0:c2:c4:58:de:17:18:1f:fa:42:97:
                    b8:1e:3f:8a:6a:b7:18:66:b9:b7:f7:75:83:bd:6b:
                    83:94:b7:d6:d8:19:18:20:5f:cf:48:e2:28:87:b1:
                    d0:be:ac:84:9b:0b:e7:57:3a:f5:a1:51:8c:92:05:
                    24:73:b9:bc:cc:a4:58:ba:b7:87:66:9c:1c:83:c1:
                    2f:23:e6:15:cc:1a:df:6d:e2:0f:28:02:f8:1f:a1:
                    e1:50:81:77:1f:e2:80:72:c3:72:7c:09:13:cd:9c:
                    1b:cc:94:53:2a:69:26:41:4a:b3:f6:26:59:d6:c1:
                    39:92:10:9f:be:70:d3:23:e7
                Exponent: 65537 (0x10001)
-
-
-
```

Zdroj: http://www.ica.cz/; Budiš P. – Elektronický podpis a jeho aplikace v praxi

Každý certifikát má na obecné úrovni jistým způsobem standardizovanou podobu prostřednictvím různých doporučení. Mezi základní charakteristické znaky, které můžeme vidět i na předchozím obrázku, patří:

- *číslo certifikátu* (Serial Number), jež musí být unikátní v rámci jedné certifikační autority (jeho obdobou je číslo občanského průkazu),
- *algoritmus použitý k podpisu certifikátu certifikační autoritou* (Signature Algorithm),
- *jména vystavitele* (Issuer) *a vlastníka* (Subject),
- *platnost certifikátu*, udávaná počátkem (Not Before) a koncem (Not After) platnosti,
- neméně důležitou částí je i samotný *veřejný klíč vlastníka* (Subject Public Key Info).[15]

[15] Budiš, P. – Elektronický podpis a jeho aplikace v praxi, 2008, str. 42

Za obsah vystaveného certifikátu ručí certifikační autorita jeho podepsáním svým soukromým klíčem. Tento akt není na příkladu znázorněn z důvodu značné délky elektronického podpisu. Je tedy zřejmé, že i samotný poskytovatel certifikačních služeb musí mít zřízen certifikát. Na základě této znalosti je možné odlišit:

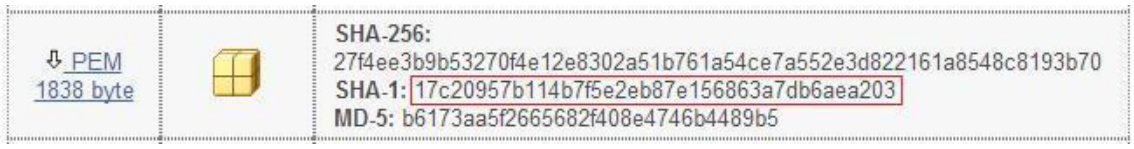
- Certifikáty poskytovatelů certifikačních služeb
- Klientské certifikáty

2.4.1.1 Certifikáty poskytovatelů certifikačních služeb

U tohoto konkrétního druhu je největším problémem zjištění důvěryhodnosti konkrétního certifikátu. Může to být zajištěno dvěma způsoby. Důvěryhodnější z nich je zřízení další nadřazené instituce mající za úkol vydávání certifikátů přímo certifikačním autoritám. Jako příklad je možné uvést Slovenskou republiku, kde tento účel plní Národný bezpečnostný úrad.

Druhou možností je vydání vlastního tzv. *kořenového certifikátu*. Jeho spolehlivost musí být následně zajištěna buď bezpečným přenosem mezi komunikujícími stranami, nebo „zveřejněním takového certifikátu prostřednictvím důvěryhodného prostředníka.“[16] Tímto prostředníkem je v České republice Ministerstvo vnitra. V praxi toto porovnání probíhá porovnáním hashe certifikátu s jeho zveřejněnou verzí. Tento proces je možné vidět na následujících obrázcích.

Obrázek 6 Hash kořenového certifikátu První certifikační autority dle oficiálního webového portálu



Zdroj: http://ica.cz/[17]

[16] Budiš, P. – Elektronický podpis a jeho aplikace v praxi, 2008, str. 46
[17] http://ica.cz/SHA2-Kvalifikovany

Obrázek 7 Hash kořenového certifikátu První certifikační autority dle Ministerstva vnitra České republiky

Poř. číslo	Ověření kvalifikovaného systémového certifikátu poskytovatele	
	Subjekt	Adresa
16.	První certifikační autorita, a.s. identifikační číslo 26 43 93 95	Podvinný mlýn 2178/6, PSČ 190 00 Praha 9
Certifikát má platnost od 1.9.2009.		
Výsledky ověření		
A.	Jméno: qica_root_key_20090901.pem	Délka: 1838 byte
	Formát certifikátu	Otisk
	PEM SHA-1	17C2 0957 B114 B7F5 E2EB 87E1 5686 3A7D B6AE A203
	MD5	B617 3AA5 F266 5682 F408 E474 6B44 89B5

Zdroj: http://www.mvcr.cz/[18]

I tyto specifické certifikáty mají omezenou dobu platnosti, která se pohybuje obvykle v rozmezí 5 a více let. Pro ověření certifikátu je tedy důležité, aby v jakémkoli okamžiku jeho platnosti, byl platný i certifikát certifikační autority. Je patrné, že doba do konce platnosti musí být minimálně stejně dlouhá u certifikátu certifikační autority jako u posledního vydaného klientského certifikátu.

2.4.1.2 Klientské certifikáty

Certifikáty tohoto druhu jsou již podkladem pro použití elektronických podpisů jednotlivými právnickými a fyzickými osobami. Z hlediska úrovně zabezpečení a regulace je možné rozlišovat dva konkrétní typy certifikátů.

- *Komerční*

Nejsou upravené zákonem. Elektronický podpis na jejich základě je tedy možné využít například pro šifrování datového přenosu, podepisování dokumentů, autentizaci a podobně. Tohoto typu jsou i *serverové certifikáty*, využívající se například při identifikaci webových serverů. Neoznačují tedy osobu nebo společnost, ale server.

[18] http://www.mvcr.cz/clanek/e-podpis-povinne-zverejnovane-informace-vysledky-overeni-platnych-kvalifikovanych-systemovych-certifikatu-akreditovanych-poskytovatelu-certifikacnich-sluzeb.aspx

- *Kvalifikované*

Jsou upravené a definované zákonem č. 227/2000 Sb., o elektronickém podpisu, a vydávané pouze kvalifikovanými certifikačními autoritami. Dle tohoto právního předpisu mohou být použity pouze za účelem elektronického podepisování dokumentů.

V této kapitole byl pojem *certifikační autorita* mnohokrát zmíněn. Je však nutné jej podrobněji rozebrat pro ucelené pochopení problematiky.

2.4.2 Certifikační autorita

„Certifikační autoritou může být kdokoliv, kdo přijímá žádosti o certifikát, ověřuje, vydává, obnovuje, zneplatňuje a zveřejňuje seznam zneplatněných certifikátů.“[19] Je možné ji vytvořit i v rámci společnosti pouze jako interní oddělení. Avšak certifikáty jí vydané za těchto podmínek nebudou mít vně podniku téměř žádnou váhu, pokud společnost není spolehlivá a nemá dostatečnou ekonomickou sílu přesvědčit obchodní partnery o jejich důvěryhodnosti.

Aby certifikační autorita získala veřejné uznání důvěryhodnosti a jí vydané certifikáty mohly být použity bez předchozí domluvy obou stran a uznány i z hlediska právní platnosti, musí být splněny určité podmínky[20]. Pouze za předpokladu, že veškeré tyto požadavky splňuje, je možné označit takovou certifikační autoritu za *kvalifikovaného poskytovatele certifikačních služeb*. Podle zákona o elektronickém podpisu má nad kvalifikovanými certifikačními autoritami dohled Ministerstvo vnitra České republiky, které také zveřejňuje jejich seznam (viz níže).

[19] Čermák, M. – Základy kryptografie pro manažery: certifikační autorita, 15. 5. 2011
[20] Specifikovány v České republice v zákoně č. 227/2000 Sb., o elektronickém podpisu a vyhlášce č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb.

Obrázek 8 Seznam kvalifikovaných certifikačních autorit

Ministerstvo vnitra zveřejňuje v souladu s § 9 odst. 2, písm. e) zákona č. 227/2000 Sb.

Poř. číslo	Poskytovatelé certifikačních služeb	Kvalifikované služby	Zahájení vydávání
1.	První certifikační autorita, a. s., identifikační číslo 26 43 93 95, Podvinný mlýn 2178/6, PSČ 190 00 Praha 9	Vydávání kvalifikovaných certifikátů; Vydávání kvalifikovaných systémových certifikátů; Vydávání kvalifikovaných časových razítek.	03/2002 02/2006 02/2006
2.	Česká pošta, s. p., identifikační číslo 47 11 49 83, Olšanská 38/9, PSČ 225 99 Praha 3	Vydávání kvalifikovaných certifikátů; Vydávání kvalifikovaných systémových certifikátů; Vydávání kvalifikovaných časových razítek.	09/2005 04/2005 07/2009
3.	eIdentity a. s., identifikační číslo 27 11 24 89, Vinohradská 184/2396, PSČ 130 00 Praha 3	Vydávání kvalifikovaných certifikátů; Vydávání kvalifikovaných systémových certifikátů; Vydávání kvalifikovaných časových razítek.	08/2005 08/2005 08/2010

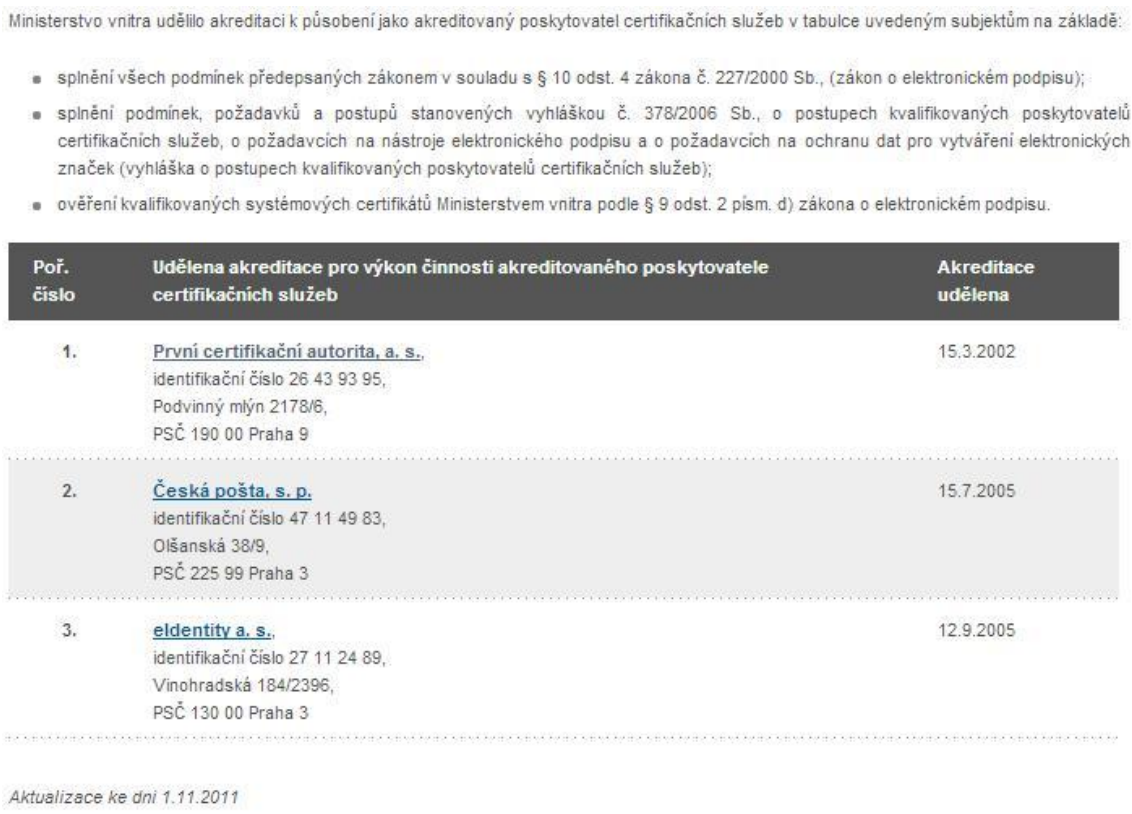
Odbor Hlavního architekta eGovernment, 1. 8. 2012

Zdroj: http://www.mvcr.cz/[21]

Avšak ani elektronický podpis založený na kvalifikovaném certifikátu od poskytovatele této úrovně nemůže být použit při styku se státní správou. Aby toho bylo docíleno, musí certifikační autorita získat od Ministerstva vnitra tzv. *akreditaci*. Podmínky pro její udělování a akreditované certifikační autority je možné vidět na výňatku z webových stránek Ministerstva vnitra níže.

[21] http://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb-320051.aspx

Obrázek 9 Seznam akreditovaných certifikačních autorit



Ministerstvo vnitra udělilo akreditaci k působení jako akreditovaný poskytovatel certifikačních služeb v tabulce uvedeným subjektům na základě:

- splnění všech podmínek předepsaných zákonem v souladu s § 10 odst. 4 zákona č. 227/2000 Sb., (zákon o elektronickém podpisu);
- splnění podmínek, požadavků a postupů stanovených vyhláškou č. 378/2006 Sb., 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);
- ověření kvalifikovaných systémových certifikátů Ministerstvem vnitra podle § 9 odst. 2 písm. d) zákona o elektronickém podpisu.

Poř. číslo	Udělena akreditace pro výkon činnosti akreditovaného poskytovatele certifikačních služeb	Akreditace udělena
1.	První certifikační autorita, a. s., identifikační číslo 26 43 93 95, Podvinný mlýn 2178/6, PSČ 190 00 Praha 9	15.3.2002
2.	Česká pošta, s. p. identifikační číslo 47 11 49 83, Olšanská 38/9, PSČ 225 99 Praha 3	15.7.2005
3.	eIdentity a. s., identifikační číslo 27 11 24 89, Vinohradská 184/2396, PSČ 130 00 Praha 3	12.9.2005

Aktualizace ke dni 1.11.2011

Zdroj: http://www.mvcr.cz/[22]

Je tedy možné s jistotou říci, že v České republice všichni kvalifikovaní poskytovatelé certifikačních služeb získali akreditaci.

Certifikační autorita jakéhokoli typu plní několik různých funkcí vyplývajících z výše zmíněných skutečností. Je možné je rozdělit do čtyř kategorií[23]:

- *Autentizace a registrace ostatních certifikačních autorit a uživatelů.*
- *Uložení a distribuce dat.* Jedná se především o certifikáty, seznamy zneplatněných certifikátů a citlivé údaje o jejich vlastnících.
- *Vydávání certifikátů a certifikační správní funkce.*
- *Notářské funkce.* Do této kategorie spadají činnosti související s oběhem elektronických dokumentů (např. jejich předání, zpracování a archivace).

Vyplývá tedy potřeba vysokého zabezpečení jak fyzických, tak softwarových přístupů k datům. Nejvíce chráněným bývá soukromý klíč samotné certifikační autority. Důvod je prostý, při jeho odcizení by mohl pachatel vytvářet falešné elektronické

[22] http://www.mvcr.cz/clanek/prehled-udelenych-akreditaci.aspx
[23] Budiš, P. – Elektronický podpis a jeho aplikace v praxi, 2008, str. 70

podpisy pod jakýmkoli smyšleným jménem. Jedním z častých zajištění je tzv. HSM (Hardware Security Module) v podobě samostatného zařízení s přístupem po síti. Nespornou výhodou je, že v případě pokusu do něj „násilně vniknout, dochází k jeho samozničení a tím je zničen i privátní klíč certifikační autority.“[24]

2.5 *Časová razítka*

Z důvodu omezené platnosti certifikátu je nutné znát přesný časový údaj vzniku elektronického podpisu. Ten je zanesen již do jeho kódu při jeho vytvoření. Nicméně je získán ze systémových hodin počítače, kde proběhl proces podepsání. Pro zabezpečení věrohodnosti okamžiku vytvoření elektronického podpisu či samotného dokumentu je proto nezbytné využít tzv. *časového razítka*.

Časová razítka jsou obdobnou službou jako vydání certifikátu k elektronickému podpisu. Jejich prostřednictvím je možné zaručit důvěryhodné „přiřazení aktuálního časového údaje k existujícím datům, informacím, souborům nebo událostem.“[25] Využívají se tedy v takových případech, kdy je vysoká pravděpodobnost nutnosti ověření existence dokumentu či elektronického podpisu v budoucnu. Konkrétním příkladem může být archivace účetních dokladů v elektronické podobě (detailní rozbor této problematiky je možné nalézt dále v této práci). Aby však jakékoli dokumenty mohly být právně uznatelné, je nutné využití z hlediska zabezpečení silnější formy, a to tzv. *kvalifikovaného časového razítka*, které by mělo obsahovat nejméně:

- unikátní číslo kvalifikovaného časového razítka,
- označení pravidel, podle kterých bylo kvalifikované časové razítko vydáno,
- časový údaj, jehož odchylka nepřesáhne 1 sekundu od UTC[26] (s tolerancí +/- 500 ms),
- otisk (hash) dat, pro která bylo kvalifikované časové razítko vydáno,
- elektronickou značku časové autority, která kvalifikované časové razítko vydala.[27]

[24] Čermák, M. – Základy kryptografie pro manažery: certifikační autorita, 15. 5. 2011
[25] http://www.ica.cz/Podrobny-popis-sluzby
[26] Universal Time Coordinated
[27] http://www.ica.cz/Podrobny-popis-sluzby

Je možné si všimnout zmíněné podobnosti s certifikátem elektronického podpisu. Přesto se však jedná o samostatnou službu, která je poskytována *časovými autoritami* (často jsou součástí certifikační autority). Z vyjmenovaných náležitostí kvalifikovaného časového razítka si lze všimnout hlavního rozdílu oproti certifikátu. V případě časového razítka se nejedná o identifikaci osoby spojené s jejím veřejným klíčem, ale o spojení identity dokumentu (hashe) a časového údaje určující okamžik, před kterým tento dokument existoval. Z této skutečnosti vyplývá, že každé časové razítko má pouze jednorázové použití pro konkrétní dokument, oproti elektronickému podpisu, který je možné použít neomezeně po určenou časovou dobu danou platností certifikátu. Ovšem i garance platnosti časového razítka je omezená. Její délka se liší dle časové autority, jež tuto službu poskytuje (3 – 6 let).[28]

[28] Peterka, J. – Báječný svět elektronického podpisu, 2011

3 Silné a slabé stránky elektronického podpisu

Oproti vlastnoručnímu podpisu má ten elektronický velké množství výhod. Avšak i přes značnou snahu vlády a odborné veřejnosti o jeho zdokonalení, stále má i mnoho nedostatků. Některé z těchto aspektů byly již naznačeny. Podrobnější rozbor silných a slabých stránek je uveden v následujících podkapitolách.

3.1 Výhody elektronického podpisu

Elektronický podpis stejně jako vlastnoruční plní některé základní funkce. Pokud je založen na kvalifikovaném certifikátu, pak představuje neodvolatelný právní úkon. Ze samotné podstaty unikátnosti dvojice klíčů ve spojení s certifikátem identifikuje vlastníka podpisu. Navíc však oproti písemnému podpisu zajišťuje, že zpráva či dokument nebyl po jeho podepsání následně pozměněn. Vyplývá to z hlavního rozdílu mezi elektronickým a vlastnoručním podpisem. Neboli z hlediska jejich samostatné existence. Vlastnoruční podpis může existovat sám o sobě, například pokud osoba podepíše prázdný list papíru, její podpis se nezmění bez ohledu na to, zda ho někdo vystřihne nebo nad něj něco připíše. Na platnosti podpisu se přitom nic nemění. Zatímco elektronický podpis má pokaždé jinou podobu, jak již bylo vysvětleno v kapitole *Elektronický podpis*.

V tomto bodě je nutno poznamenat, že většina lidí, a mezi nimi i někteří uživatelé elektronického podpisu si tuto poslední funkci vykládají jako zaručení nezměnitelnosti či dokonce nečitelnosti originálu. I když využití elektronického podpisu pro zašifrování celé zprávy není vyloučené, v běžné praxi se tento způsob nevyužívá, jak již bylo zmíněno dříve, z důvodu náročnosti procesu asymetrické kryptografie na výpočetní výkon.

Další významnou výhodou je možnost podepsat, či lépe řečeno zašifrovat, cokoli co existuje v elektronické formě. Může tím být jakýkoli soubor od jednoduchého textového formátu TXT, přes emaily a audiovizuální data až po komplexní programy. Podepsat je možné nejen samostatné objekty, nýbrž i jejich oběh, tedy datový přenos.

Předností je také jednoduché ověření jeho pravosti. U vlastnoručního podpisu je nutné jeho zkoumání a porovnávání s podpisovým vzorem zkušeným odborníkem

(grafologem). [29] Elektronický podpis, respektive certifikát, na němž je založen, je často ověřován pouze jednou, a to prostou kontrolou platnosti u certifikační autority. Po ujištění se o jeho důvěryhodnosti je certifikát přidán v počítači do skupiny důvěryhodných, a následně veškeré dokumenty opatřené elektronickým podpisem pod tímto certifikátem jsou automaticky zpracovávány a po bezkonfliktním porovnáním hashů považovány za bezpečné a věrohodné.

3.2 Nevýhody elektronického podpisu

Na prvním místě je nutné uvést ne přímo nevýhodu, avšak spíše překážku pro větší rozšíření používání elektronického podpisu veřejností. A to nejen podnikatelskou sférou ale i soukromou. Touto překážkou je nedostatečná informovanost osob o podstatě a podobě elektronického podpisu a jeho nesporných výhodách. Jak již bylo ukázáno v předchozích kapitolách na několika příkladech, stále je velké množství lidí, jež nemají ani základní znalosti o elektronickém podpisu. Mezi nimi jsou i tací, kteří přestože pracují ve společnostech využívajících této služby, tak nevědí, že ji jako zaměstnanci používají na denní bázi. Je to způsobeno tím, že algoritmy pro podepisování jsou zapracované v samotném programovém vybavení počítačů a používány automaticky bez nutnosti zaškolení zaměstnanců.

Samotné použití elektronického podpisu a jeho ověření je tedy jednoduché. Problémem je však jeho zřízení. Zajištění kvalifikovaného certifikátu je komplikovaný proces, vyžadující vyplnění online žádosti, prokázání své totožnosti, zaplacení poplatku, pořízení čtečky a čipové karty a přidání certifikátu certifikační autority do důvěryhodných. Administrativní náklady mohou být tak vysoké, že u některých podnikatelů převáží přínosy, které by tím získali.

Značná nevýhoda elektronického podpisu se skrývá v rychlém technologickém pokroku. Je to dáno ze dvou důvodů. Jedním je podstata asymetrické kryptografie, která pracuje pouze s omezenou výpočetní kapacitou. Jelikož odvození veřejného klíče od privátního je založeno na matematickém modelu, pak není nemožné její prolomení, ale dosažení tohoto cíle v racionálním čase. Je tedy zřejmé, že doba použitelnosti současných šifrovacích algoritmů je závislá především na tempu vývoje nových a rychlejších zařízení a jejich prolomení je pouze otázkou času. Tento problém se týká

[29] Peterka, J. – Co je elektronický podpis?, deník Právo, 4. 5. 2000

i hashovacích algoritmů. Z těchto důvodů je také časově omezena platnost certifikátů. S technologickým posunem je proto nutné souběžně vyvíjet stále nové a komplexnější metody šifrování a používání klíčů vycházejících z čísel stále vyššího řádu.

V návaznosti na tento pokrok je možné zmínit druhou slabinu, která se netýká přímo elektronického podpisu, nýbrž zabezpečení prostředků pro jeho použití. Privátní klíč může být uložen na různých paměťových médiích jako je USB flash disk nebo čipová karta. Z těchto dvou možností se považuje čipová karta jako nejbezpečnější způsob, jelikož veškeré operace probíhají přímo na ní. Je proto velmi nepravděpodobné odcizení samotného soukromého klíče bez karty. Ovšem použití čipové karty nezabraňuje neoprávněnému zneužití. Pro vysvětlení nejlépe poslouží následující příklad.

> *Na počítač uživatele se dostane nějakým způsobem speciálně připravený škodlivý kód. Tento program by pak na pozadí sledoval zapojení čtečky, přítomnost čipové karty. Většina karet bývá dalším způsobem zabezpečena například PIN kódem. Toto heslo by po jeho zadání program zaregistroval. Po získání těchto informací by „vyzval" čipovou kartu pro potvrzení předem připraveného hashe dokumentu. Jelikož by se prokázal platným heslem PIN, čipová karta by vytvořila elektronický podpis. Výsledkem by byla naprosto legitimní transakce platná a jako taková by představovala neodvolatelný právní úkon. To vše na jméno vlastníka čipové karty, který by se o této transakci mohl dovědět až po určité době.*[30] [31]

Z příkladu je zřejmé, že ani maximálním zabezpečením prostředků pro tvorbu elektronických podpisů není možné zajistit jejich nezneužití. Určité snížení tohoto rizika je možné prostřednictvím různé antivirové ochrany počítačů, avšak i výrobci těchto obran přiznávají, že některé viry neodhalí dříve než po několika letech.[32]

Další důležitou slabou stránkou je jednoznačně právní úprava. V minulosti byl tento fakt ještě významnější, a to do roku 2004, kdy byla vydána novela zákona o elektronickém podpisu. Přesto některé nedostatky jsou v tomto zákoně přítomny dodnes, a dle slov některých odborníků další nejasnosti jsou přidávány s každou

[30] Nápravník, J. – Jsou čipové karty bezpečné?, LUPA.cz, 27. 3. 2006
[31] Na tento problém pan Jiří Nápravník znovu upozorňuje i ve svém článku pro server root.cz pod názvem „Časovaná bomba jménem (ne)zaručený elektronický podpis" ze dne 14. 6. 2013.
[32] Kaspersky Lab Expert - The "Red October" Campaign, SECURELIST, 14. 1. 2014

aktualizací. Toto je způsobeno především snahou vlády o zapracování evropských směrnic do legislativy České republiky s co nejmenším prodlením.

Významnou nevýhodou elektronického podpisu je také omezená platnost certifikátu. Nejčastěji se jedná o období jednoho roku. Každá kvalifikovaná certifikační autorita je ze zákona povinna vést seznamy jí vydaných a zneplatněných certifikátů. Z elektronického podpisu jako takového však není možné určit, zda byl dokument podepsán v době jeho platnosti. Z toho důvodu se začala využívat *časová razítka* popsaná v jedné z předchozích kapitol.

4 Legislativní úprava

Aby mohl být elektronický podpis využíván i mimo interní prostředí firmy, je samozřejmě nutné určit všeobecně přijímaná pravidla a záruky. Ty zajišťuje právní úprava. Historie legislativy byla již rozebrána v úvodní kapitole této diplomové práce. Tato část je zaměřena na současné právní předpisy v Evropské unii, České republice a jejich slabá místa.

4.1 Evropská unie

Základním právním předpisem v rámci Evropské unie upravujícím elektronické podpisy je směrnice 1999/93/EC, o zásadách Společenství pro elektronické podpisy. Obsahem tohoto dokumentu jsou mimo jiné definice základních pojmů, vymezení povinnosti členských států z hlediska zapracování této směrnice do jednotlivých legislativních rámců, provádění dohledu nad certifikačními autoritami, určení právní účinnosti elektronických podpisů, odpovědnosti a ochrany dat.

Pro úplnost je také důležité zmínit rozhodnutí Komise 2009/767/ES[33] upravující použití a přijímání elektronických podpisů, jejímž účelem bylo odstranění nedostatků bránících bezproblémovému vzájemnému uznávání kvalifikovaných certifikátů v Evropské unii.[34] Právě tato směrnice zavedla povinnost vedení tzv. *seznamů důvěryhodných služeb* (TSL).

Významnou změnu uvádí rozhodnutí Komise 2011/130/EU. Tímto právním předpisem byly zavedeny referenční formáty elektronických podpisů (BES a EPES). Všechny členské státy tak musí zavést veškeré nezbytné technické prostředky pro zajištění jejich bezproblémového zpracování. Účelem tohoto kroku je snadná a spolehlivá přeshraniční komunikace mezi jednotlivými státy Evropské unie.

V současné době je také v projednávání návrh nařízení Evropského parlamentu a Rady. Podnětem byla především zastaralost obsahu směrnice 1999/93/EC. Toto nařízení by již mělo výrazněji zasahovat do používání elektronického podpisu, avšak bez nutnosti úpravy legislativy jednotlivých členských zemí. Obsahem nařízení je aktualizace základních pojmů a úprava elektronické identifikace, dohledu nad poskytovateli důvěryhodných služeb, právní účinek elektronického podpisu,

[33] Toto rozhodnutí Komise bylo později novelizováno formou rozhodnutí Evropské komise 2010/758/EU.
[34] www.mvcr.cz/clanek/novela-rozhodnuti-komise-2009-767-es.aspx

elektronických značek, časového razítka, elektronických dokumentů a elektronického doručování, a další.

4.2 Česká republika

Základním právním předpisem, který upravuje elektronický podpis v České republice je zákon č. 227/2000 Sb., o elektronickém podpisu. Již byl mnohokrát aktualizován. Tímto právním předpisem je elektronický podpis rozlišován na třech úrovních důvěryhodnosti. Po základní definici elektronického podpisu následuje výčet kriterií, jež musí splňovat k dosažení vyšší formy zmiňované již v předchozích kapitolách, a to *zaručeného elektronického podpisu.*

Na nejvyšším stupni důvěryhodnosti z pohledu tohoto zákona stojí tzv. *uznávaný elektronický podpis*. Do legislativy České republiky byl zanesen v souladu s výše uvedenou směrnicí 2011/130/EU ze dne 25. února 2011. Jsou jím veškeré zaručené elektronické podpisy založené na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb či poskytovatelem certifikačních služeb, který má sídlo mimo území České republiky a je uveden v seznamech důvěryhodných služeb (TSL = Trusted Services List).[35] Elektronická značka je zde definována obdobným způsobem avšak pouze ve dvou úrovních důvěryhodnosti:

- *Elektronická značka*, která je vymezena z hlediska důvěryhodnosti na stejné úrovni jako zaručený elektronický podpis
- *Uznávaná elektronická značka*, jež je ekvivalentem uznávaného elektronického podpisu.

Tento zákon také mimo dalších pojmů vymezuje povinnosti podepisující případně označující osoby, kvalifikovaných poskytovatelů certifikačních služeb, odpovědnost za škodu, ochranu osobních údajů, udělování akreditací, náležitosti kvalifikovaného certifikátu, zneplatnění kvalifikovaného certifikátu, uznávání zahraničních kvalifikovaných certifikátů a prostředky pro vytváření elektronických podpisů a značek.

[35] Pro ověření je možné využít stránek provozovaných Ministerstvem vnitra České republiky – http://tsl.gov.cz/certiq

Elektronický podpis a věci s ním související samozřejmě upravují i další právní předpisy. Například zákon č. 2/1969 Sb.[36], který stanovuje Ministerstvo vnitra České republiky jako instituci zodpovědnou za dohled, vývoj a regulaci nad certifikačními autoritami a elektronickým podpisem. Dále vyhláška č. 378/2006 Sb. určující postupy kvalifikovaných poskytovatelů certifikačních služeb, požadavky na nástroje elektronického podpisu a požadavky na ochranu dat pro vytváření elektronických značek. Elektronický podpis je také zapracován do jiných právních předpisů. Jedná se mimo jiné o zákon č. 89/2012 Sb., občanský zákoník, zákon č. 563/1991 Sb., o účetnictví, zákon č. 499/2004 Sb., o archivnictví a spisové službě, zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů a vyhláška 212/2012 Sb.

4.3 Slabé stránky současné právní úpravy v České republice

Tato kapitola upozorňuje na některá nejasná místa v současné právní úpravě elektronického podpisu v České republice. Především se jedná o nesrovnalosti ve významových definicích některých základních pojmů.

Jako první je nutné upozornit na rozdíl mezi *elektronickým* a *digitálním* podpisem. Chápané jsou jako synonyma s geografickým rozdílem v použití. Pojem digitální podpis je ukotven v legislativě Spojených států amerických, oproti elektronickému podpisu v rámci Evropské unie. Obecné definice přívlastků digitální a elektronický tyto dva pojmy však odlišují.

Digitálními je možné označit jakákoli data vyjádřená v binární soustavě. Mohou být ale reprezentována různými technologiemi například v elektronické (počítače), optické (optické kabely), opticko-mechanické (CD, DVD), či mechanické (děrné štítky) podobě apod.. Typickým znakem je dokonale přesná konverze týchž dat mezi jednotlivými podobami.

Jak vyplývá z předchozího vysvětlení, je nezbytné zanést do právní úpravy elektronického podpisu přesnou definici, která by termín elektronický podpis stavěla na roveň digitálního podpisu. Zákon č. 227/2000 Sb., jež je zanesením směrnic Evropské unie do české právní úpravy, však specifikuje elektronický podpis jako „údaje v elektronické podobě“. Tato nejasnost je navíc součástí tohoto předpisu již od jeho

[36] Zákon o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky

vstupu do účinnosti v roce 2000. [37] A to i přesto, že dle slov pana Peterky[38] „návrh zákona vypracovaný odbornou skupinou, toto omezení na elektronickou podobu dat neobsahovalo.“[39] Z této definice také vyplývá, že elektronickým podpisem může být cokoli, co je prostředkem pro „jednoznačné ověření identity podepsané osoby ve vztahu k datové zprávě.“ Otázkou tedy zůstává, zda pod tento pojem spadá například i vlastnoruční podpis převedený do elektronické podoby naskenováním.

Další problém se skrývá pod výkladem pojmu *zaručený elektronický podpis*, který je definován výčtem vlastností, jež musí splňovat. Elektronický podpis tedy musí:

- „být jednoznačně spojen s podepisující osobou,
- umožnit identifikaci podepisující osoby ve vztahu k datové zprávě,
- být vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
- být k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoli změnu dat.“

Z takto vyjádřené definice je zřejmé, že zaručeným elektronickým podpisem je jakýkoli elektronický podpis založený na certifikátu, tak jak je prezentován v této diplomové práci. Nutno však upozornit na absenci specifikace míry důvěryhodnosti certifikátu tímto zákonem. Logicky je možné vyvodit, že přívlastek „zaručený“ se týká pouze zajištění rozpoznání jakékoli změny dokumentu provedené po jeho podepsání. V této podobě ho ale nelze považovat za právně závazný, jelikož nesplňuje nezbytný základní požadavek, a tím je nepopiratelnost. Ta je splněna až vydáním kvalifikovaného certifikátu k tomuto elektronickému podpisu. Některé internetové zdroje však zaručený elektronický podpis vysvětlují způsobem vyvolávající představu automatického splnění této podmínky. Nutno podotknout, že tuto podmínku v určitých případech opomíjela i právní úprava, a to až do novelizace účinné od 1. července 2012.

Takovýchto nedostatků by bylo jistě možné najít při podrobnějším rozboru daného zákona více. Velkou překážkou pro hromadné použití elektronického podpisu veřejností je, dle odborníků, zanášení nových diskutabilních nařízení společně

[37] Peterka, J. – Názvoslovné omyly světa počítačů, Novinky, 17. 2. 2000
[38] Pan Peterka byl součástí skupiny nezávislých odborníků pověřené uskupením SPIS a Úřadem pro státní informační systém pro vytvoření návrhu zákona o elektronickém podpise, který byl následně v upravené formě schválen a od kterého se tato skupina později veřejným prohlášením distancovala.
[39] Peterka, J. – Elektronický podpis

s upřesněním stávajících vymezení. Příkladem může být novela zákona o elektronickém podpisu č. 167/2012 Sb., která ve své podstatě ukládá osobě komunikující s orgány veřejné správy a nepoužívající formátů předem určených směrnicí 2011/130/EU, zapracované i do tohoto zákona, povinnost zpřístupnění „k neomezenému a bezplatnému užití způsobem umožňujícím dálkový přístup aplikaci, která umožní okamžité ověření uznávaného elektronického podpisu nebo uznávané elektronické značky.“[40] Praktickou aplikaci tohoto požadavku v současné době splňuje pouze služba Secustamp, která však není bezplatná, pracuje pouze se soubory ve formátu PDF a je schopna ověřit pouze platnost podpisového certifikátu.

[40] § 11 odst. 5 písm. b) zákona č. 227/2000 Sb., o elektronickém podpisu ve znění pozdějších předpisů

5 Využití elektronického podpisu v účetnictví

Obecný princip elektronického podpisu má mnoho využití nejen v podnikatelské nýbrž i v soukromé sféře. Je možné ho například využít v situacích, kdy vyvstane potřeba šifrování dat, určení autora informací, zaručení neporušitelnosti i v mnoha dalších. Z hlediska účetnictví jsou mezi nejrozšířenějšími oblastmi využívání služeb elektronického podpisu především elektronická fakturace, využití pro interní účely, komunikace s orgány státní správy a samosprávy a archivace účetních dokladů.

5.1 Elektronická fakturace

Je možné rozlišovat dva druhy fakturace. Buď prostřednictvím tištěného, nebo elektronického účetního dokladu. Stále se lze v praxi setkat se situací, kdy papírové faktury jsou odeslány poštou odběrateli, u něhož následně zodpovědný pracovník tyto faktury zaúčtuje. Tento proces je však vysoce neefektivní.

Druhou možností, jež je používaná nejčastěji, je nahrazení fyzického přenosu faktury elektronickým prostřednictvím emailové zprávy a faktury například ve formátu PDF podepsané elektronickým podpisem nebo elektronickou značkou založenou na kvalifikovaném certifikátu. U příjemce zprávy je doklad vytištěn a zaměstnancem zadán do účetního systému. Tento způsob však skrývá nebezpečí. Pokud účetní jednotka nemá prostředky nebo nechce takovýto doklad archivovat v elektronické formě, pak je nutná jeho konverze pouze zákonem předepsaným způsobem[41] pro zamezení znehodnocení elektronického podpisu. Tato povinnost se netýká dokumentů, u kterých ani jedna ze stran nezpochybní proces jejich převodu a dokumentů specifikovaných zákonem o archivnictví a spisové službě.[42] Podrobnější rozbor spolehlivé konverze dokumentů je uveden dále v kapitole *Archivace účetních dokladů*.

Zmíněné způsoby fakturace mezi obchodními partnery jsou však velice neefektivní s poměrně vysokou pravděpodobností výskytu chyby. Je to způsobeno hlavně zapojením lidského faktoru do zpracování každého dokladu. Ideálním případem je absence tohoto slabého místa. Na řešení pracují odborné organizace již dlouhou dobu.

V praxi se zažilo nejprostší řešení tzv. *EDI* (Electronic Data Interchange) spočívající v předávání elektronických faktur ve standardizovaném a strukturovaném

[41] § 33 zákona č. 563/1991 Sb., o účetnictví ve znění pozdějších předpisů
[42] Zákon č. 499/2004, o archivnictví a spisové službě ve znění pozdějších předpisů

formátu. Systém obou stran je díky němu schopen po přijetí účetního dokladu jej automaticky přečíst a zaúčtovat. K prosazení této komunikace je však nutná buď určitá míra finančního a ekonomického vlivu jedné společnosti nad ostatními, nebo dohoda jednotlivých stran. Důvodem jsou značné náklady při zavádění této technologie.

V České republice pro zajištění určitého obecně přijatelného a volně dostupného formátu vzniklo dne 26. ledna 2010[43] sdružení ICT Unie sloučením sdružení SPIS a APVTS (Asociace provozovatelů veřejných telekomunikačních sítí). Významným aktem v historii SPISu bylo podepsání *Deklarace o společném postupu v oblasti řešení elektronické fakturace v ČR*. Jejím předmětem byl závazek 14 různých předních výrobců ekonomických a ERP systémů vybudovat společný formát elektronické fakturace a následně implementovat do svých produktů.[44] Na tomto základě byl vytvořen strukturovaný formát ISDOC umožňující automatizované zpracování elektronických faktur.

V současné době v České republice bohužel stále převažuje zasílání elektronických faktur mezi obchodními partnery prostřednictvím emailu. Tento důsledek je zároveň pravděpodobně i příčinou tohoto problému. Jelikož naše ekonomika je postavena především na malých a středních firmách, které nemusí mít dostatečné finance na zajištění investice do technických zařízení nutných pro využití elektronické fakturace, případně náklady na pořízení vysoce převýší jejich výnosy z nich plynoucí.

Nicméně není nutné se omezovat na elektronickou fakturaci. Elektronickou cestou a s pomocí elektronického podpisu založeného na kvalifikovaném certifikátu je možná výměna jakýchkoli dokumentů (např. objednávek, konfirmací, bankovních výpisů, apod.) či emailových zpráv se zaručením identity odesilatele, zachování integrity dat a nepopiratelnosti.

5.2 Interní využití

Využití v interním prostředí firmy nebo holdingu je již z logiky věci nespočetně více. Jelikož není nutná tak vysoká míra zabezpečení, jako v případě přímé komunikace s obchodními partnery, každá společnost má možnost dát přednost využití komerčnímu před kvalifikovaným certifikátem při ověřování platnosti elektronického podpisu.

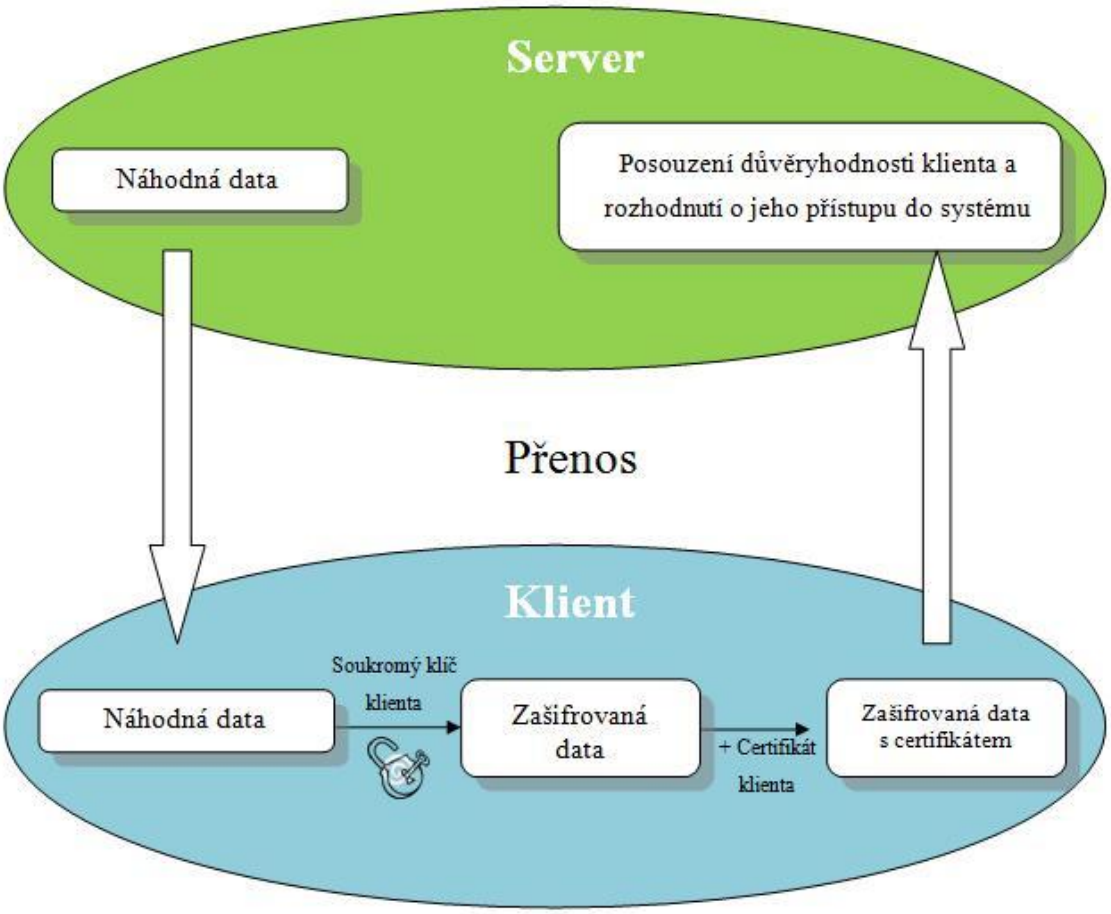
[43] Server ITBIZ, 29. 1. 2010, www.itbiz.cz/vznik-ict-unie
[44] ISDOC, www.isdoc.cz

Jak již bylo vysvětleno v kapitole *Certifikační autority*, certifikáty si může vydávat pro své interní účely sama společnost a tím se vyhnout nákladům na jeho pořízení a obnovu od kvalifikovaného poskytovatele certifikačních služeb. Mohou však narůst požadavky na zabezpečení jejich databáze a s nimi spojené dodatečné investiční náklady.

Ve spojení s předchozí podkapitolou vyplývá jedno použití pro interní účely firmy, a to pro víceúrovňové schvalování dokumentů. Jako příklad může sloužit vystavení objednávky, která je v první řadě sestavena na základě odpovědným zaměstnancem podepsaného požadavku z výrobního oddělení. Tento dokument následně přechází ke schválení nákupnímu oddělení, které vystaví a podepíše koncept objednávky. Tu poté schválí například finanční ředitel a podepíše svým zaručeným elektronickým podpisem založeným na komerčním certifikátu a uznávanou elektronickou značkou společnosti.

Hlavním účelem používání elektronického podpisu v rámci jedné společnosti je jistě nahrazení přihlašovacího jména a hesla. Zabezpečení prostřednictvím těchto údajů je v dnešní době již považováno za nedostatečné a z hlediska autentizace za nejslabší. Přesto je při jejich nahrazení nutné certifikáty registrovat a spárovat s jednotlivými účty oprávněných osob v systémech společnosti. Samotné ověřování identity probíhá dvojím způsobem.

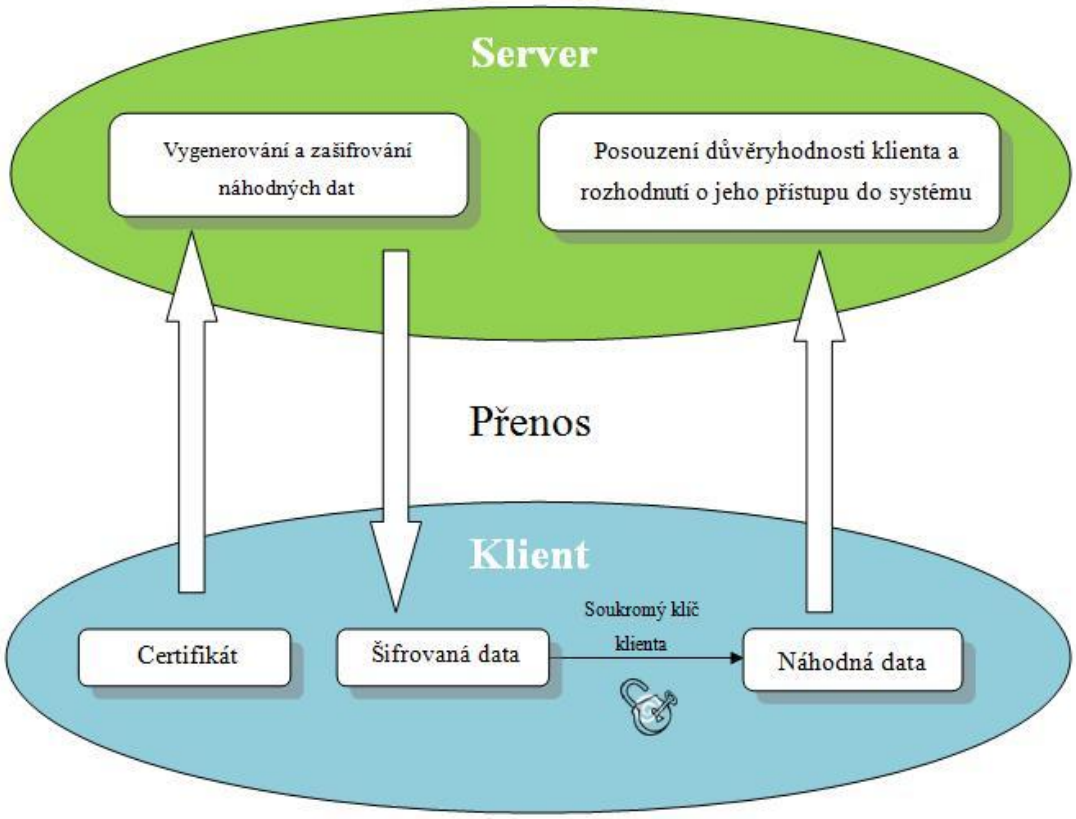
Obrázek 10 První princip autorizace klienta při přihlašování do informačního systému



Zdroj: Vlastní zpracování

Jak je možné vidět i na předchozím schématu, tak v prvním případě nejprve server odešle náhodný datový řetězec na počítač přihlašující se osoby, která tato data následně zašifruje svým soukromým klíčem a společně s certifikátem odešle pro ověření serveru. Ve druhé situaci je serveru nejprve zaslán certifikát, pomocí veřejného klíče v něm obsaženého je uzamknut obdobný datový řetězec jako v prvním případě a zaslán nazpět přihlašující se osobě. Ta svým soukromým klíčem tento elektronický podpis odemkne a vrátí zpět serveru, který provede ověření.

Obrázek 11 Druhý princip autorizace klienta při přihlašování do informačního systému



Zdroj: Vlastní zpracování

V praxi se z těchto dvou způsobů používá ten první. Pro úplnost je nutno podotknout, že takovéto přihlašování probíhá až po navázání zabezpečené komunikace například protokolem SSL (který také čerpá z principů asymetrické kryptografie). [45]

Pokud bychom navázali na takovýto způsob přihlašování, tak by bylo možné využít výhod, jež poskytuje elektronický podpis i při dodržování následné dohledatelnosti původních účetních záznamů po jejich změně. V takovém to případě by se oprávněná osoba přihlásila do účetního systému a zaúčtovala libovolný účetní případ. Software by po provedení této akce účetní záznam automaticky podepsal soukromým klíčem osoby obsaženým na USB flash disku nebo čipové kartě, čímž by se zaručila identifikace osoby a zachovaná integrita záznamu. Při jakékoli změně by se pouze přidal další podpis. Otázkou zůstává, zda tento stupeň zabezpečení není nadbytečně složitý a časově náročný pro použití v běžných situacích.

[45] Peterka, J. – Báječný svět elektronického podpisu, 2011

Dva způsoby interního použití principů elektronického podpisu, s nimiž je možné setkat se v praxi nejčastěji, jsou pak *podepisování a šifrování emailových zpráv* a tvorba *virtuální privátní sítě* (VPN = Virtual Private Network).

Podepisování emailových zpráv je jednoduché a ve většině případů zahrnuje pouze stisknutí jediného tlačítka. Pokud například nějaký zaměstnanec společnosti potřebuje zaslat třetí straně zprávu s citlivými informacemi, je nezbytné ji nějakým způsobem zašifrovat. K tomu lze využít veřejný klíče příjemce. Provedení tohoto kroku se samozřejmě neobejde bez certifikátu adresáta, který musí být předem doručen buď samostatně, nebo součástí jiné dříve přijaté a elektronicky podepsané zprávy.

Pro dálkový přístup zaměstnanců k zabezpečeným serverům společnosti je možné využít tzv. *Virtual Private Network*. Název vychází ze skutečnosti, že se jedná o soukromou síť s regulovanými přístupovými právy, která však pracuje virtuálně prostřednictvím internetu. Proces zabezpečení v nejjednodušší formě probíhá následovně:

- „klient nejprve zašle požadavek serveru o navázání komunikace,
- server tuto žádost vyhodnotí a zašle klientovi svůj certifikát,
- klient po ověření platnosti certifikátu vygeneruje dočasný tajný klíč, zakóduje ho prostřednictvím veřejného klíče serveru a odešle nazpět,
- obě strany ve finálním kroku využijí dočasného tajného klíče pro odvození řádného tajného klíče, kterým šifrují vzájemnou komunikaci.“[46]

5.3 Komunikace s orgány státní správy a samosprávy

Jedním z hlavních důvodů pořizování elektronického podpisu založeného na kvalifikovaném certifikátu vydaném akreditovanou certifikační autoritou je v praxi jednoznačně možnost elektronické komunikace s orgány státní správy a samosprávy. Jako příklad použití je možné uvést:

- zasílání elektronických podání různým úřadům prostřednictvím e-podatelen,
- podávání daňových přiznání,

[46] Volně převzato: Peterka, J. – Báječný svět elektronického podpisu, 2011, str. 411

- zasílání dokumentů ČSSZ (České správě sociálního zabezpečení),
- při žádostech o dotace z EU,
- při žádostech o výpisy z obchodních rejstříků,
- zasílání zpráv prostřednictvím *datových schránek*,
- a další.[47]

5.3.1 Datové schránky

Pod pojmem *datová schránka* si lze představit poštovní schránku pro elektronické dokumenty primárně určenou pro komunikaci s orgány veřejné moci. Jako takové jsou součástí *Informačního systému datových schránek* (ISVS). Jsou definovány v § 2 odst. 1 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů jako „elektronické úložiště, které je určeno k

a) doručování orgány veřejné moci,
b) provádění úkonů vůči orgánům veřejné moci,
c) dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob.“

Vlastní zřizování a správu datových schránek má v rámci České republiky ve své pravomoci Ministerstvo vnitra. Provoz však zajišťuje státní podnik Česká pošta. Dle zmíněného právního předpisu mají všechny fyzické osoby bez ohledu na to, zda podnikají či nikoli, a všechny právnické osoby nárok na bezplatné zřízení jedné datové schránky. Advokátům, daňovým poradcům a insolvenčním správcům je zřízena datová schránka automaticky v momentě jejich zapsání do zákonem stanovené evidence. Totéž platí pro právnické osoby zřízené zákonem v momentě jejich vzniku a právnické osoby zapsané v obchodním rejstříku ve chvíli jejich zápisu do této evidence.

Využívání této služby je povinné při komunikaci:

- dvou orgánů veřejné správy navzájem,
- orgánu veřejné správy vůči fyzickým či právnickým osobám, kterým byla zřízena datová schránka.

Datové schránky mají několik nesporných výhod. První je jejich garance provozovatele za doručení zprávy. Zákon v takovémto případě stanovuje, že pokud

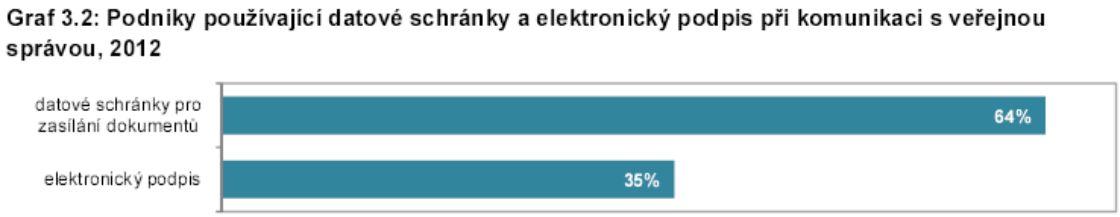
[47] www.ica.cz/Elektronicky-podpis

zpráva nebyla přečtena do deseti dnů od vložení do datové schránky, považuje se za doručenou. Další jednoznačnou výhodou je šifrování veškerých přijatých dat a tím zajištění důvěrnosti přenášených zpráv. Oproti klasickému předání dokumentů emailem datové schránky automaticky využívají elektronického podpisu s certifikátem ISDS. Každá zpráva procházející datovou schránkou je tak elektronicky podepsána s přiloženým kvalifikovaným časovým razítkem.

Slabou stránkou je omezená velikost souboru, jež je možné do schránky odeslat, přestože její kapacita je neomezená. Není také možné uložení souborů v jiných než zákonem stanovených formátech. Potenciální slabinou je i celkové zabezpečení veškerých dat, jelikož jsou zašifrovány na základě certifikátu, který si vydává sama Česká pošta prostřednictvím své certifikační autority PostSignum. Je tedy diskutabilní zabezpečení „proti chybě nebo záměrné manipulaci provozovatele systému samotného.“[48]

Na následujícím grafu je možné vidět podíl společností využívajících datových schránek (64 %) a elektronického podpisu (35 %) při komunikaci s veřejnou správou.

Obrázek 12 Podíl podniků využívajících elektronický podpis a datové schránky při komunikaci s veřejnou správou za rok 2012



Zdroj: Dotazníkový průzkum Českého statistického úřadu z roku 2013

5.3.2 E-podatelny a Daňový portál

S orgány státní správy a samosprávy lze tedy komunikovat prostřednictvím datových schránek. Pokud však fyzická či právnická osoba žádnou nevlastní a nezažádá o její zřízení, pak mohou využít tzv. *e-podatelen*. Nejčastěji se jedná o založenou emailovou schránku vyhrazenou pouze pro tyto účely (např. Vláda České republiky)[49],

[48] Smejkal, V., Valášek, M. – Jak na datové schránky: Praktický manuál pro každého, 2012, str. 170
[49] http://www.vlada.cz/cz/urad-vlady/elektronicka-podatelna/elektronicka-podatelna-16034/

ale může se jednat i o komplexní webové stránky (např. portál Ministerstva spravedlnosti České republiky)[50]. Ze zákona je stanovena povinnost jejího zřízení pro každou organizaci státní správy. Požadavky na zasílání a podobu elektronických podání se liší dle provozovatele každé e-podatelny. Nicméně ve všech případech je vyžadováno opatřit datovou zprávu uznávaným elektronickým podpisem nebo přihlášení do webové služby pomocí kvalifikovaného certifikátu vydaného akreditovanou certifikační autoritou.

Za specifický typ e-podatelny lze označit i *daňový portál*, sloužící pro podávání různých písemností vůči orgánům Finanční správy. Provozovatelem této služby je Generální finanční ředitelství. Převážně se jedná o úplná elektronická daňová přiznání, které mohou být podány touto cestou několika způsoby:

- „podepsané uznávaným elektronickým podpisem,
- odeslané prostřednictvím datové schránky, nebo
- s ověřenou identitou podatele způsobem, kterým se lze přihlásit do jeho datové schránky.“[51]

Pro využití první možnosti je nutné využít uznávaný elektronický podpis založený na kvalifikovaném certifikátu obohaceném o tzv. *identifikátor MPSV*[52]. Poslední bod je pak využitelný až od 1. ledna 2014, kdy nabylo účinnosti opatření Senátu č. 344/2013 Sb., o změně daňových zákonů v souvislosti s rekodifikací soukromého práva a o změně některých zákonů. Zmiňovaný předpis dále stanovuje souběžné zřízení *daňové informační schránky* se zřízením datové schránky. Důležité je podotknout, že daňový portál umožňuje zasílat některé typy písemností neopatřené uznávaným elektronickým podpisem.

5.4 *Archivace účetních dokladů*

Využívání elektronických účetních dokladů má mnoho výhod i pár nedostatků. Vážnější problémy nastávají především při jejich archivaci. V případě klasických papírových dokladů nemůžeme hovořit o nějakých zásadnějších překážkách. V dnešní době je možné se setkat se situacemi, kdy archivaci papírových dokladů podnik

[50] http://epodatelna.justice.cz/
[51] § 71 odst. 1 zákona č. 280/2009 Sb., daňový řád ve znění pozdějších předpisů
[52] Identifikátor MPSV označuje jedinečnou identifikaci osoby vůči Ministerstvu práce a sociálních věcí, Finančnímu úřadu, České správě sociální zabezpečení a Úřadu práce České republiky.

přenechává jiné firmě, která se na tuto činnost specializuje. Archivace elektronických dokumentů všeobecně je však mnohem složitější. Sice je možné využít autorizované konverze a převést doklady z elektronické do papírové formy, ale tato metoda je značně nákladná, a pokud je dokument v jiném formátu než PDF či PDF/A, tak ji ze zákona ani nelze využít.

Na nejzákladnější úrovni se požadavky na elektronický doklad neliší od požadavků na doklad v papírové formě. Dokument v obou případech musí splnit mimo jiné tato kritéria:

- Dostupnost
- Čitelnost
- Pravost

Díky pokročilým technologiím není v dnešní době problém s dostupností elektronických dokladů. Existuje spousta formátů pro strukturované i nestrukturované dokumenty.

Z nejdůležitějších požadavků při archivaci účetních dokladů je jejich čitelnost fyzickou osobou. Za předpokladu, že v takové formě nejsou vedené, musí osoba zodpovědná za archivaci disponovat prostředky pro převod do patřičné podoby. Jedná se např. o, již v dnešní době nepoužívaný, floppy disk. Většina dokladů se musí archivovat po velmi dlouhou dobu. V případě např. účetní závěrky je to 10 let. U papírových dokladů to není žádný problém, i když pro jejich skladování jsou nutné prostory, metody jejich řazení pro snadné vyhledávání, dodatečné náklady a různá bezpečnostní opatření. Naproti tomu elektronické doklady nejenže se zachycují na různých paměťových mediích, ale navíc se s technologickým vývojem mění i softwarem podporované formáty. Všechny dokumenty se tedy dříve či později stanou ve své původní podobě nečitelnými, a s vysokou pravděpodobností ještě před vypršením doby archivace.

Pro dlouhodobou archivaci je proto nezbytné tento nedostatek řešit použitím jedné z následujících tří základních metod:

- Emulace
- Virtualizace
- Migrace

Emulace v tomto pohledu znamená, že novější systém vytvoří prostředí vnímané starými soubory jako jejich domovské prostředí. Tato technologie má však své limity, které často znemožňují její použití v praxi. Existují například případy, kdy nezávisí jen na systému, ale také na dalším softwarovém vybavení počítače.

Virtualizace není nic jiného než použití některého základního jazyka nepodléhajícího změnám i přes různé generace programového vybavení počítačů.

Třetí a současně v dnešní době pohlížené jako nejpřijatelnější metodou je migrace. Jedná se o proces založený na konverzi dat ze starého a nepodporovaného formátu do formátu nového. Nicméně tento proces je stále problémový. Je-li příslušný dokument opatřen elektronickým podpisem, pak integrita dokumentu je zajišťována až na úrovni bitů a je tedy logické, že při konverzi je tato integrita narušena a elektronický podpis ztrácí svou hodnotu. Řešením může být „užití důvěryhodné instituce, která migraci provede s tím, že sice budou porušeny původní bezpečnostní mechanismy dokumentu, ale při migraci vzniknou nové, vytvořené dostatečně důvěryhodnou a nezpochybnitelnou institucí.“[53]

Dle zákona 499/2004 Sb., o archivnictví a spisové službě, se dokument považuje za pravý, „byl-li podepsán platným uznávaným elektronickým podpisem nebo označen platnou elektronickou značkou osoby, která k tomu byla v okamžiku podepsání nebo označení oprávněna, osoby odpovědné za převedení z dokumentu v analogové podobě nebo změnu formátu dokumentu v digitální podobě nebo osoby odpovědné za provedení autorizované konverze dokumentů a opatřen kvalifikovaným časovým razítkem.“ Z toho vyplývá, že každý doklad musí být před archivací zkontrolován, zda obsahuje platné kvalifikované časové razítko a zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaným akreditovanou certifikační autoritou, a platnost těchto aspektů musí být prokázána i kdykoli později. Z důvodu omezené platnosti certifikátů je nutné časové razítko neustále obnovovat, a to ještě před vypršením platnosti předchozího (princip digitální kontinuity). Za situace, kdy elektronický doklad nebude přerazítkován, musí být v době jeho platnosti protokolárně uložen na nepřepisovatelném médiu či převeden do papírové formy.

Prokázání pravosti je důležité především pro daňové doklady z důvodu potřeby zajištění nepopiratelnosti, oproti archiváliím obecně, kde je nejdůležitějším požadavkem

[53] Budiš, P. – Elektronický podpis a jeho aplikace v praxi, 2008, str. 145

čitelnost a zachování integrity dokumentu. Je to z toho důvodu, že význam jako archiválie může mít i falzifikát.

V souvislosti s dlouhodobou archivací elektronických dokumentů se stává velice vážným problémem elektronického podpisu i stárnutí použitých algoritmů. Je například možné, že v budoucnu budou dostupné postupy i výpočetní kapacita pro odvození privátního klíče od veřejného. Dále je potřebné řešit případy, kdy certifikát sloužící k ověření elektronického podpisu a časového razítka již není dostupný, není dostupná informace o jeho zneplatnění či v situaci, kdy vypršel nebo byl odvolán z důvodu krádeže certifikátu. Řešením je pak přikládat jednotlivé průkazní záznamy k dokumentům.

V dnešní době již existují řešení na mnohé z těchto problémů. K vyhnutí se komplikacím s čitelností dokumentů je dobré využívat formáty jednodušší, které nepodléhají častým změnám a nejsou spojeny jen s jedním výrobcem či technologií. Jedná se například o prostý textový formát TXT nebo formát PDF/A, který byl i přijat jako standard ISO. Klasický PDF nezaručí správné zobrazení dat v jakékoli verzi softwarových nástrojů. PDF/A tím, že splňuje následující předpoklady, tento nedostatek odstraňuje:

- „nezávislost na platformě
- všechny informace potřebné pro správné zobrazení jsou uvnitř souboru (například fonty, definice barev apod.)
- veškerá metadata jsou ve formátu XMP
- žádné šifrování, žádná ochrana hesly apod.
- žádný audio nebo video obsah
- žádný JavaScript nebo spustitelné spouštěče souborů
- nepoužívá se LZW komprese“[54]

Formát XMP (eXtensible Metadata Platform) je založený na jazyce XML a umožňuje vkládat do souborů metadata. Byl vynalezen, stejně jako formát PDF, firmou Adobe a podporuje ho i velké množství ostatního programového vybavení počítače. LZW komprese je pak univerzální bezztrátový kompresní algoritmus navržený pro rychlou implementaci.

[54] http://cs.wikipedia.org/wiki/PDF/A

Veškeré požadavky (kromě čitelnosti) na elektronické dokumenty jsou upraveny v normách vydaných Evropským institutem pro standardy v telekomunikacích (ETSI = European Telecomunications Standards Institute), ale také již v české legislativě, a to především v zákoně č. 227/200 Sb., o elektronickém podpisu a 499/2004 Sb., o archivnictví a spisové službě. Od 1. 7. 2012, kdy nabyla platnosti novela těchto zákonů, jsou i u nás v těchto zákonech zavedeny normy ETSI, které definují následující tři skupiny formátů:

- „PAdES (PDF Advanced Electronic Signatures) hovoří o připojování elektronického podpisu k PDF dokumentům.
- CAdES (Cryptographic Message Syntax Advanced Electronic Signatures) definují požadavky na elektronické podepisování dokumentů v libovolném formátu.
- XAdES (XML Advanced Electronic Signatures) hovoří o elektronickém podepisování XML dat.“[55]

Pro potřeby dlouhodobé archivace jsou důležité především formáty PAdES LTV (Long Term Validation), CAdES-A (Archival) a XAdES-A .Orgány veřejné moci jsou navíc dle této novely povinny vést spisovou službu pouze v elektronické podobě.

Tyto skupiny formátů ve své podstatě definují tři požadavky na elektronické dokumenty:

- „k dokumentu mají být připojeny všechny informace potřebné pro prokázání jeho pravosti, včetně CRL listiny z doby prvního ověření;
- dokument i tyto ověřovací atributy budou chráněny společným kontrolním otiskem, tedy elektronickým podpisem podle specifikace PAdES LTV nebo CAdES LTV;
- k takto chráněnému dokumentu budou pravidelně připojována časová razítka tak, aby nikdy nebyla přerušena jeho digitální kontinuita a aby byl vždy použit nejsilnější dostupný šifrovací algoritmus.“[56]

[55] https://www.602.cz/files/Svet602_2012_web.pdf?sid=3290
[56] https://www.602.cz/files/Svet602_2012_web.pdf?sid=3290

6 Praktická část

Na následujících stranách je uvedena praktická část této diplomové práce. Jejím předmětem je průzkum využívání elektronického podpisu v účetnictví podnikatelských subjektů o různé velikosti, právní formě, předmětu podnikání a geografické oblasti působnosti. Výzkum byl proveden prostřednictvím dotazníkového šetření.

6.1 Proces dotazníkového šetření

Samotný dotazník byl vytvořen ve dvou verzích, každá strukturována do dvou částí. Varianty se liší dle využívání či nevyužívání elektronického podpisu firmou. První pětice otázek byla všeobecného zaměření pro určení charakteru společnosti a společná pro obě verze. Zbylé otázky se již liší dle zmíněného kritéria. U respondentů nevyužívajících elektronického podpisu byly otázky č. 6 – 12 zaměřeny na důvody nevyužívání těchto služeb a jejich plány do budoucna. Na druhé straně pro podnikatelské subjekty využívající elektronický podpis byly otázky č. 6 – 24 orientovány především na oblasti, v nichž používají tuto službu a jak často, na budoucí plány a názory ohledně jejího stavu a vývoje. Dále zde bylo uvedeno několik otázek na využití služeb souvisejících s elektronickým podpisem, konkrétně na datové schránky a časová razítka. Veškeré otázky mimo prvních pěti byly volitelné.

Dotazník byl rozeslán prostřednictvím emailu. Seznam emailových adres byl stanoven pomocí náhodného výběru s kritériem právní formy společnosti z oficiálního internetového portálu Zlatých stránek[57]. Tento seznam obsahuje 586 podnikatelských subjektů. Struktura vybraných společností byla následující:

- 100 společností s ručením omezeným,
- 100 veřejných obchodních společností,
- 100 komanditních společností,
- 100 akciových společností,
- 100 družstev,
- 50 firem bylo náhodně zvoleno bez jakéhokoli kritéria,
- 36 podnikatelských subjektů specificky vybraných.

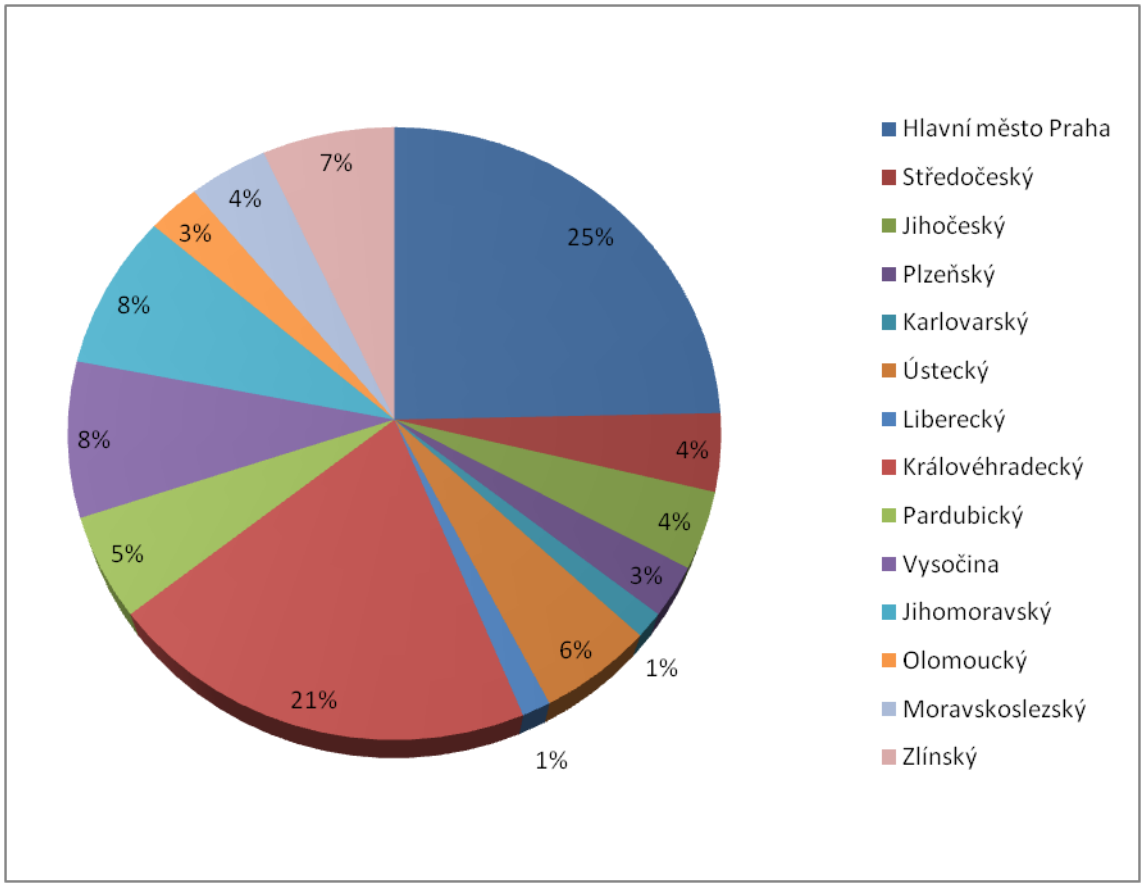
[57] http://www.zlatestranky.cz/

Z těchto rozeslaných emailů bylo úspěšně vyplněno 73 dotazníků, což činí návratnost 12,46 %. Na tomto základě se domnívám, že výsledky mohou být považovány za směrodatné a je s nimi i nadále tak pracováno při analýze výsledků. Veškeré grafy jsou vlastního zpracování, pokud není uvedeno jinak.

6.2 *Struktura respondentů dle základních charakteristik*

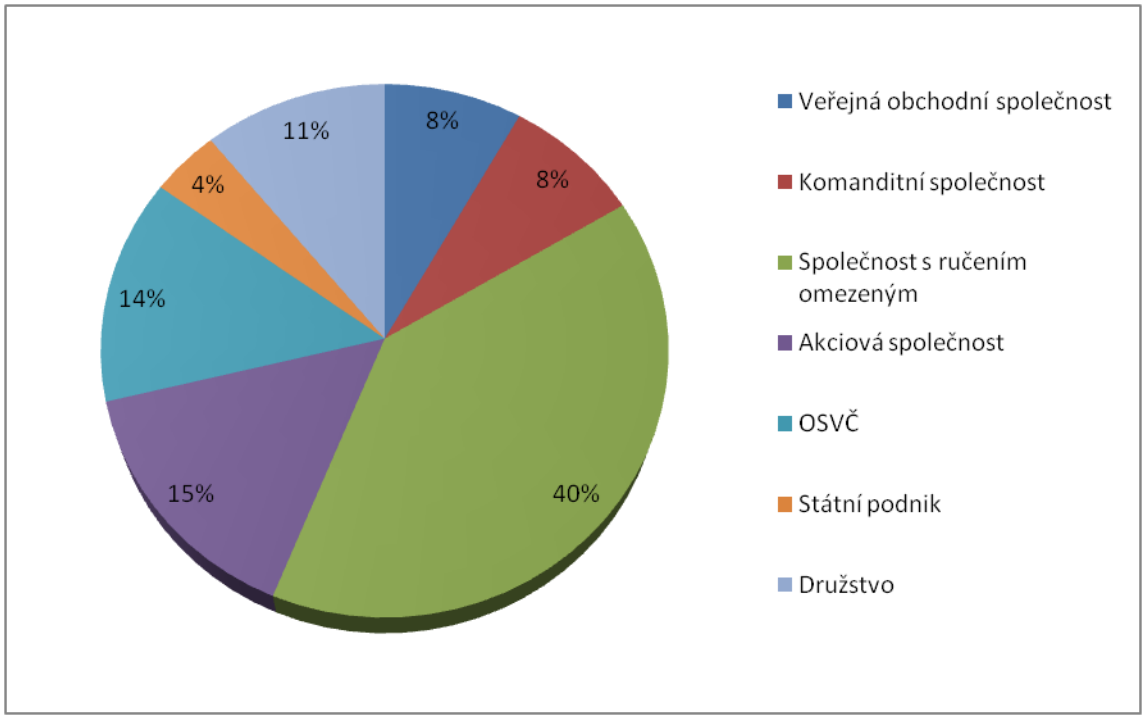
V celkovém souboru obdržených odpovědí v rozdělení dle krajů, bylo nejvíce získáno z Hlavního města Prahy (25 %) a následně z Královéhradeckého kraje (21 %). Zbývající počet odpovědí je relativně rovnoměrně rozdělen do zbývajících krajů. Tuto skutečnost znázorňuje následující graf.

Graf 1 Struktura odpovědí dle umístění sídla společnosti respondentů



Z těchto společností největší podíl měly společnosti s ručením omezeným jako právní formy, které tvořily 40 % z celkového souboru navrácených dotazníků. Následovaly akciové společnosti s 15% a OSVČ se 14% podílem.

Graf 2 Struktura odpovědí dle právní formy respondentů



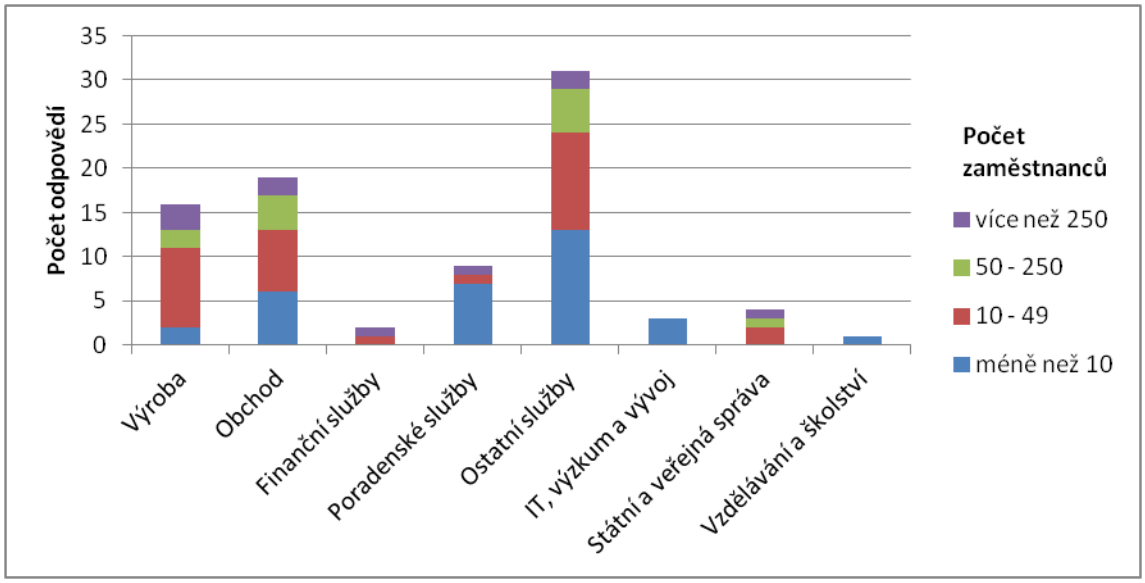
Jedním z nejdůležitějších faktorů ovlivňujícím účely a důvody rozhodnutí o pořízení či nepořízení elektronického podpisu je velikost společnosti. Pro toto kritérium, rozlišující společnosti dle počtu zaměstnanců, byly vybrány čtyři kategorie použité i při průzkumu Českým statistickým úřadem s názvem „Šetření o využívání informačních a komunikačních technologií v podnikatelském sektoru“[58]. Jedná se o následující skupiny uvedené s procentním podílem na získaných odpovědích:

- méně než 10 zaměstnanců (34,25 %),
- 10 – 49 zaměstnanců (36,99 %),
- 50 – 250 zaměstnanců (15,07 %),
- více než 250 zaměstnanců (13,7 %).

Toto rozdělení je zohledněno také v následujícím grafu zobrazujícím získané odpovědi z hlediska předmětu podnikání daných společností. Největší počet zvolených odpovědí na otázku ohledně předmětu podnikání byl u Ostatních služeb (36,47 %). Z této oblasti podnikání tvořilo 41,94 % společností s méně než 10 zaměstnanci a 35,48 % společností s 10 – 49 zaměstnanci. Druhou nejčastější oblastí podnikání byl Obchod (22,35 %) a třetí Výroba (18,82 %).

[58] http://www.czso.cz/csu/redakce.nsf/i/podnikatelsky_sektor

Graf 3 Struktura odpovědí dle předmětu podnikání a velikosti společností



Výchozí data pro sestavení tohoto grafu byla upravena. Celkový počet odpovědí na otázku předmětu podnikání je vyšší než počet navrácených dotazníků z důvodu možnosti zatrhnout více oblastí podnikání. Více než jeden obor činnosti zvolilo 12 společností, jejichž odpovědi je možné vidět v tabulce níže.

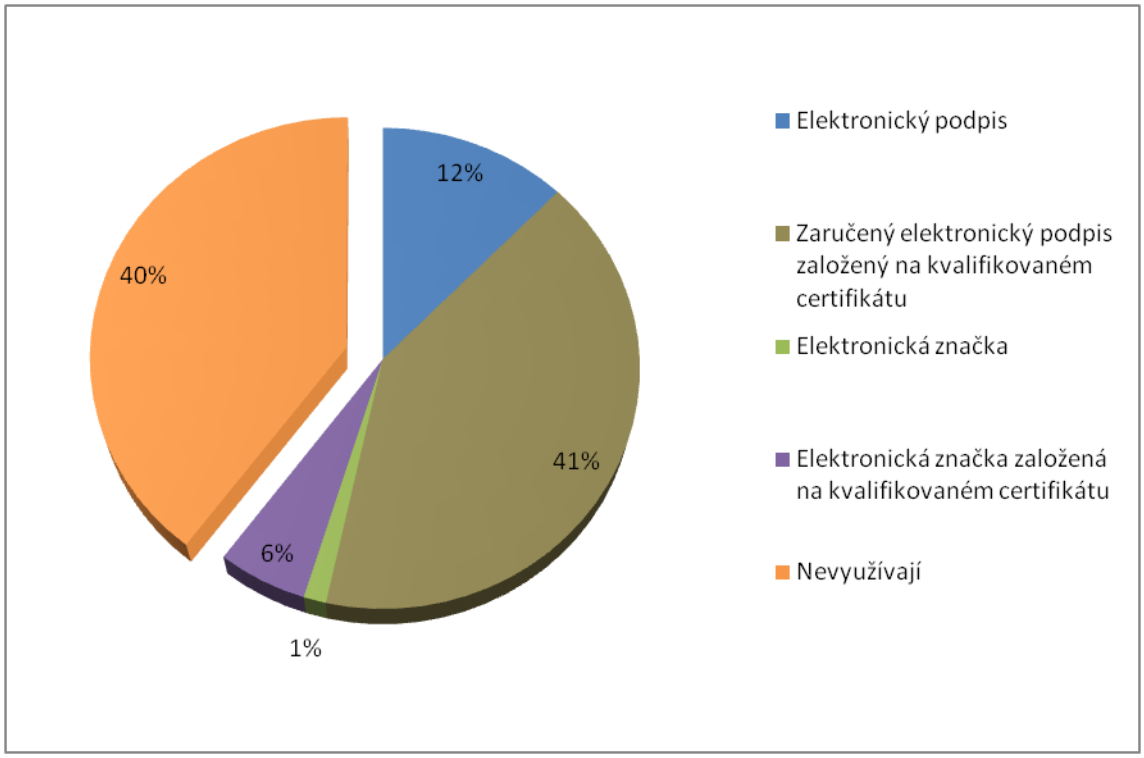
Tabulka 1 Vybrané společnosti činné ve více oborech podnikání

Obory podnikání			Počet zaměstnanců
1.	2.	3.	
Finanční služby	Státní a veřejná správa		10 - 49
Obchod	Ostatní služby		méně než 10
Obchod	Informační technologie, výzkum a vývoj		méně než 10
Obchod	Ostatní služby		10 - 49
Obchod	Ostatní služby		10 - 49
Obchod	Poradenské služby	Vzdělávání a školství	méně než 10
Ostatní služby	Informační technologie, výzkum a vývoj		méně než 10
Poradenské služby	Ostatní služby		méně než 10
Výroba	Ostatní služby		méně než 10
Výroba	Obchod		50 - 250
Výroba	Ostatní služby		10 - 49

6.3 *Analýza výsledků*

Zda konkrétní firma využívá elektronický podpis či nikoli se samozřejmě liší podle jejích potřeb a omezení. Největší vliv mají společně požadavky a ekonomická síla společnosti a jejích obchodních partnerů. S tím souvisí i kritérium velikosti firmy. Analýza výsledků dle těchto určujících faktorů je uvedena v jednotlivých podkapitolách. Obecné rozdělení odpovědí je znázorněno na grafu níže.

Graf 4 Využití elektronického podpisu dle jejich druhů

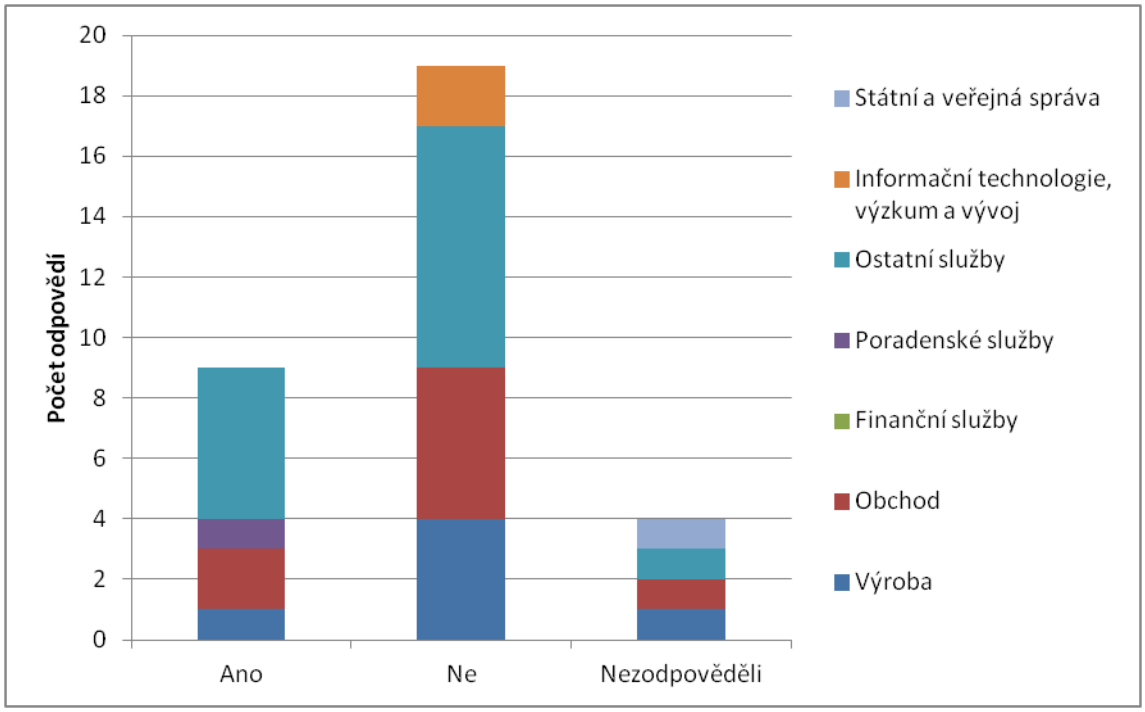


Na tuto otázku společnosti odpovídaly z hlediska jejich nejvyužívanější varianty. Z dat je možné říci, že téměř stejný počet společností využívá zaručený elektronický podpis založený na kvalifikovaném certifikátu (41,1 %) jako společností, které nevyužívají žádnou podobu této služby (39,73 %).

6.3.1 Společnosti nevyužívající elektronický podpis

V této kapitole jsou analyzovány výsledky pouze té části respondentů, která dle jejich odpovědí nevyužívá žádného typu elektronického podpisu. Jsou v celkovém počtu 29 společností, kde z 90% se jedná o malé podniky do 50 zaměstnanců. S neustálými inovacemi v poli informačních technologií, ale mnozí uvažují o jeho zavedení v budoucnu. Výsledky rozdělené dle oblastí činností jsou následovné.

Graf 5 Plány společností ohledně pořízení elektronického podpisu v budoucnu strukturované dle předmětu podnikání



V grafu je o tři odpovědi nadhodnocen sloupec společností neuvažujících o pořízení elektronického podpisu z důvodu společností s více jak jedním předmětem podnikání. Polovina respondentů (55,56 %), kteří uvažují o pořízení elektronického podpisu, podniká v oblasti ostatních služeb. Druhou skupinou pozitivně uvažující o budoucím využití této služby jsou firmy s Obchodem jako hlavní činností.

Tabulka 2 Detail specifických odpovědí respondentů z oblasti obchodu, kteří uvažují o pořízení EP

Právní forma společnosti	Počet zaměstnanců	Sídlo firmy	Účel pořízení EP	Důvod nevyužití EP v současnosti
Komanditní společnost	více než 250	Ústecký	Zasílání elektronických faktur, dodacích listů a jiných účetních dokladů Podávání daňového přiznání Zasílání datových zpráv přes datové schránky Přihlašování do systémů jako náhrada přihlašovacího jména a hesla	Nízká podpora
Společnost s ručením omezeným	10 - 49	Hlavní město Praha	Zasílání elektronických faktur, dodacích listů a jiných účetních dokladů Podávání daňového přiznání Zasílání datových zpráv přes datové schránky	zatím nebyl od nikoho požadováno zasílání dokaldů s e.p.

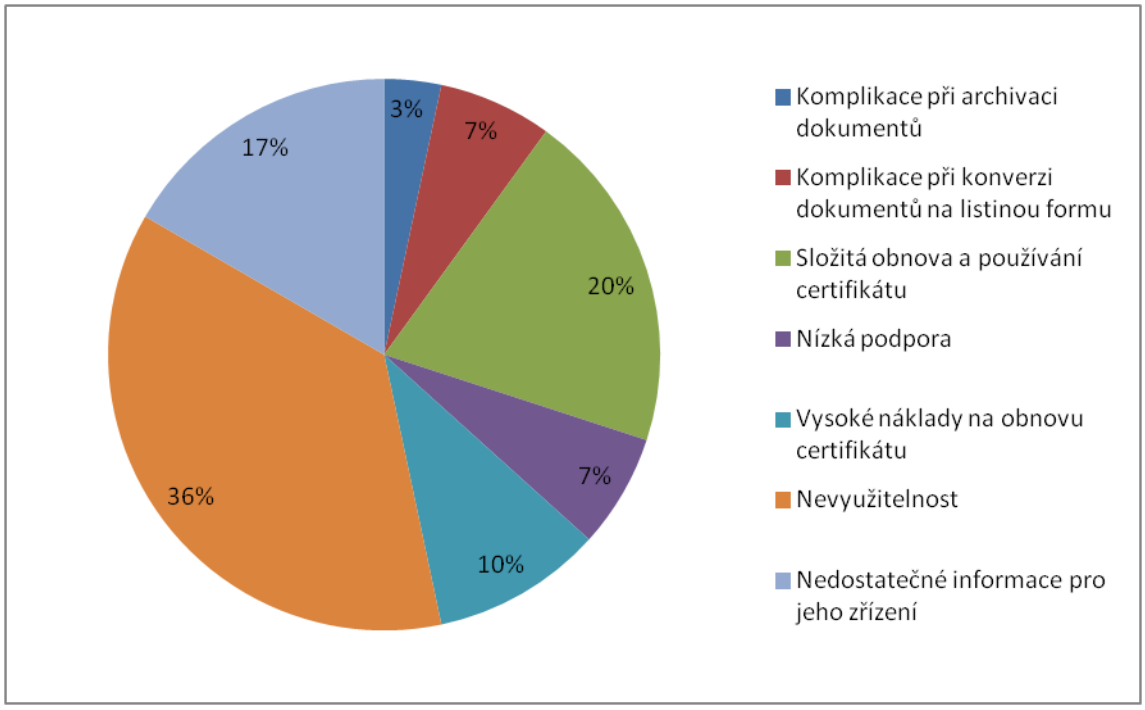
Z předchozí tabulky zobrazující některé odpovědi zmíněných dvou respondentů podnikajících v oblasti obchodu je možné vyvodit, že důvody pro zvažování jeho zřízení je v případě větší firmy úspora administrativních nákladů, avšak překážku staví

nízká podpora elektronického podpisu a nedostatek informací. Oproti tomu malá firma s 10 – 49 zaměstnanci se sídlem v Praze očekává nátlak od svých významných obchodních partnerů s větší ekonomickou silou pro jeho zavedení.

Neočekávanou odpovědí jsou dvě společnosti z oblasti IT, výzkumu a vývoje. Tito respondenti přestože vlastní technické prostředky i know-how pro bezproblémové zavedení a používání elektronického podpisu, tak neuvažují o jeho budoucím pořízení. V obou případech se však jedná o malé firmy s méně než 10 zaměstnanci. Je zřejmé, že v tomto případě by náklady na zřízení a udržování elektronického podpisu převýšily jeho přínosy.

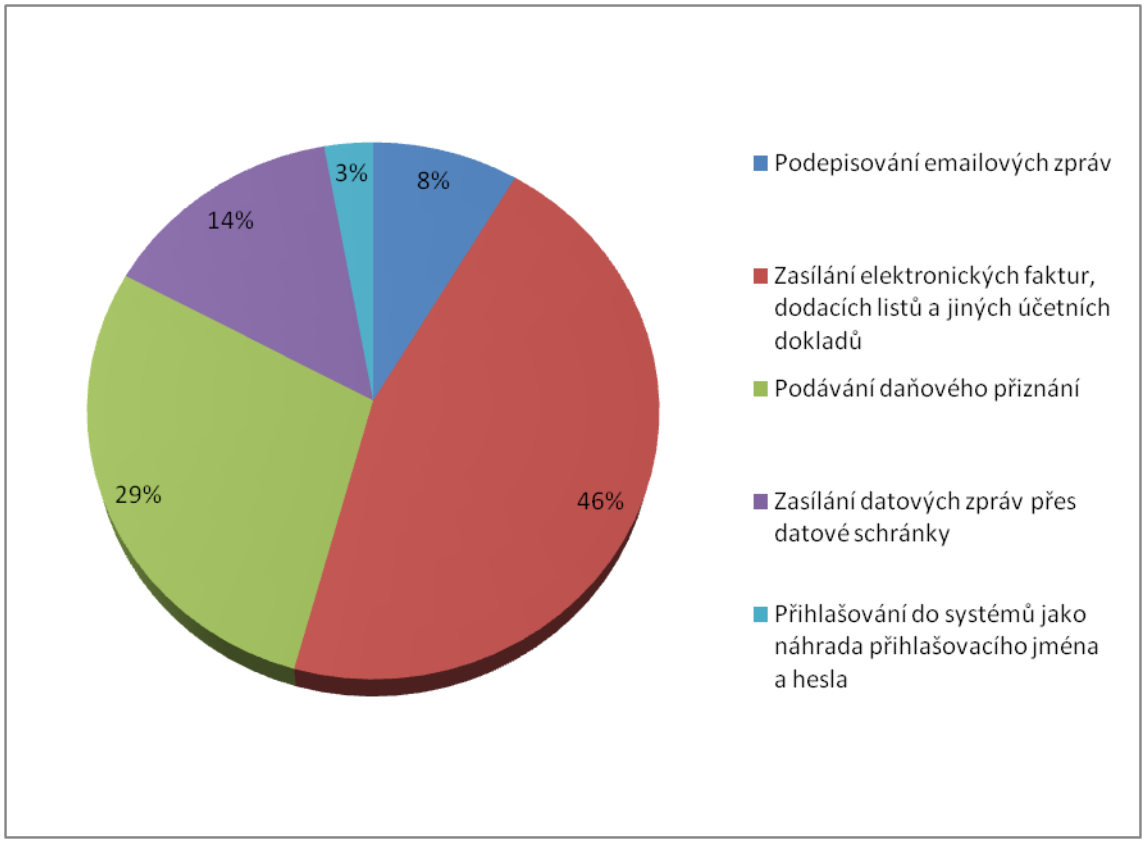
Pokud přejdeme k důvodům nevyužívání elektronického podpisu všech respondentů, je patrné, že důsledek (nevyužívání) je zároveň i příčinou tohoto problému. Více jak 36 % respondentů vyplnilo jako hlavní důvod nepořízení elektronického podpisu prostou *Nevyužitelnost* pro jejich činnost. Další významnou část odpovědí tvořily náklady na obnovu certifikátu (10 %) a složitost obnovy a používání certifikátu (20 %) a nedostatečné informace pro zřízení elektronického podpisu (16,67 %). Pro upřesnění, jediné dvě společnosti, jež mají více než 250 zaměstnanců a nevyužívají těchto služeb, uvedly jako důvod především nízkou podporu a nevyužitelnost. Tyto informace jsou lépe zobrazené na následujícím grafu.

Graf 6 Důvody respondentů pro nevyužívání EP v současnosti



Společnostem nevyužívajícím elektronický podpis byla položena otázka, z jakého důvodu by si pravděpodobně pořídily elektronický podpis, kdyby se odstranily případné překážky bránící jim v tomto rozhodnutí. Výsledky lze vidět níže.

Graf 7 Oblast využití elektronického podpisu zakládající důvod pro jeho pořízení bez ohledu na skutečný záměr společností o jeho budoucím využívání



Z celkových 29 odpovědí v této kategorii, na otázku reagovalo pouze 20 společností. Z tohoto souboru 16 by si elektronický podpis pořídilo za účelem zasílání elektronických dokumentů (45,71 %) a 10 pro podávání daňového přiznání (28,57 %). Pouze jediná firma zvolila jako jeden z hlavních důvodů pořízení přihlašování do systémů jako náhrada přihlašovacího jména a hesla. Není překvapujícím faktem, že tato firma má více než 250 zaměstnanců a jejím hlavním předmětem podnikání je Obchod.

Výsledky odpovědí na tuto otázku také potvrzují v současné době největší překážku v používání elektronického podpisu v účetnictví, kterou je archivace účetních dokladů[59]. Z této skupiny respondentů ani jeden nezvolil možnost pořízení

[59] Tuto skutečnost zobrazuje i graf 12 uvedený dále v této práci, kde z celkových 40 získaných odpovědí na využívání elektronického podpisu, 31 společností uvedlo, že na tento aspekt účetnictví jej vůbec nevyužívají.

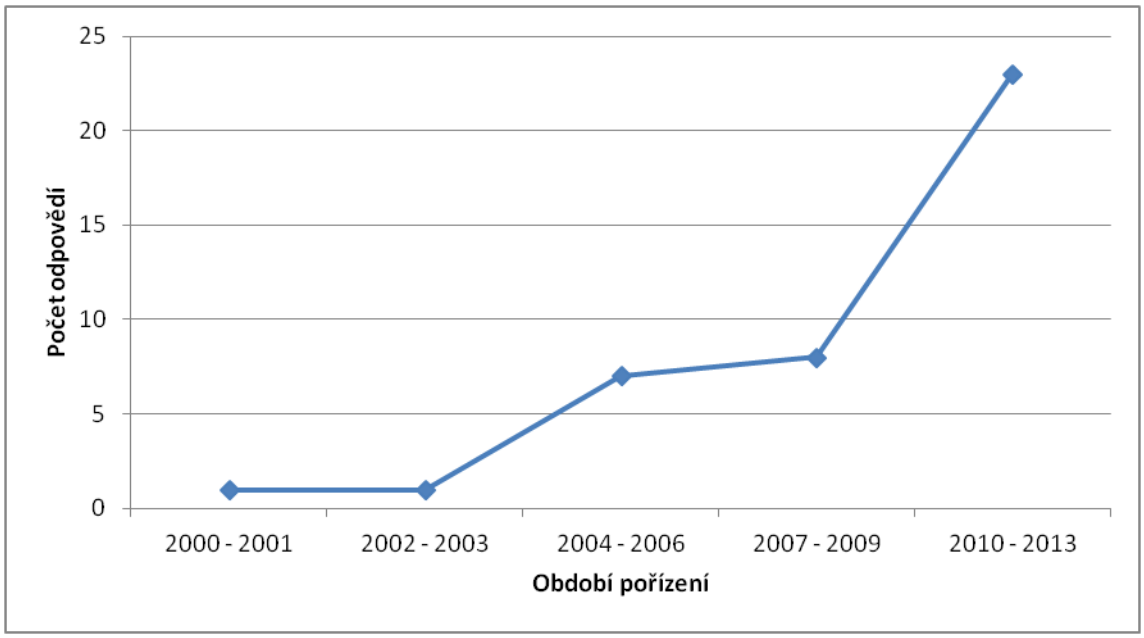
elektronického podpisu za účelem archivace dokumentů v elektronické podobě. Problematika týkající se tohoto tématu byla již rozebrána v kapitole *Archivace účetních dokladů*.

6.3.2 Společnosti využívající elektronický podpis

V této kapitole jsou již rozebrány odpovědi od společností používajících elektronický podpis o různé intenzitě a oblastech využití. Celkově se jedná o 44 společností, což činí 60,27 % z celkového počtu vyplněných dotazníků. Z těchto subjektů 86,36 % uvažují o jeho využívání nadále. Pouze dva respondenti se staví k budoucímu využívání negativně (4,55 %)[60]. Z jejich odpovědí na ostatní otázky dotazníku lze vyvodit, že možnosti využití a tudíž i přínosy elektronického podpisu při jejich podnikatelské činnosti jsou mnohem nižší než dodatečné náklady spojené s obnovou certifikátu, ale také s archivací dokumentů, které stále převádějí do písemné formy.

Dle odpovědí 40 dotazovaných firem doba, po jakou elektronický podpis používají, také koresponduje s aktualizací právní úpravy a tím také rozšiřováním možností využití.

Graf 8 Období počátku využívání elektronického podpisu



Jak je vidět na předchozím grafu, pouze dvě společnosti zavedli elektronický podpis v období od roku 2000 do roku 2003. Jak bylo zmíněno výše v kapitole

[60] Zbývající podíl 9,09 % tvoří společnosti, jež tuto otázku nezodpověděly.

Historický vývoj, v uvedeném období právní úprava byla ve svých počátcích, a zákon o elektronickém podpisu obsahoval mnoho nedostatků. Od roku 2004, kdy nabyla účinnosti novela č. 440/2000 Sb. významně měnící legislativu ohledně elektronických podpisů a jejich používání, je pak možné vidět značné navýšení jejich pořízení. Prudký nárůst pořízení elektronických podpisů zaznamenalo období 2010 – 2013. Rozšíření v tomto časovém rozmezí bylo především v oblasti velmi malých podniků do 10 zaměstnanců, které tvoří 43,48% podíl společností v těchto letech, a středně velkých s 50 – 250 zaměstnanci a podílem 34,78 %. Z následujících odpovědí je také možné usoudit, že důvodem pořízení bylo především zlepšení komunikace s orgány veřejné správy. Dokládá to i průzkum Českého statistického úřadu.

Tabulka 3 Podniky používající internet k úplnému elektronickému podání určeného pro veřejnou správu

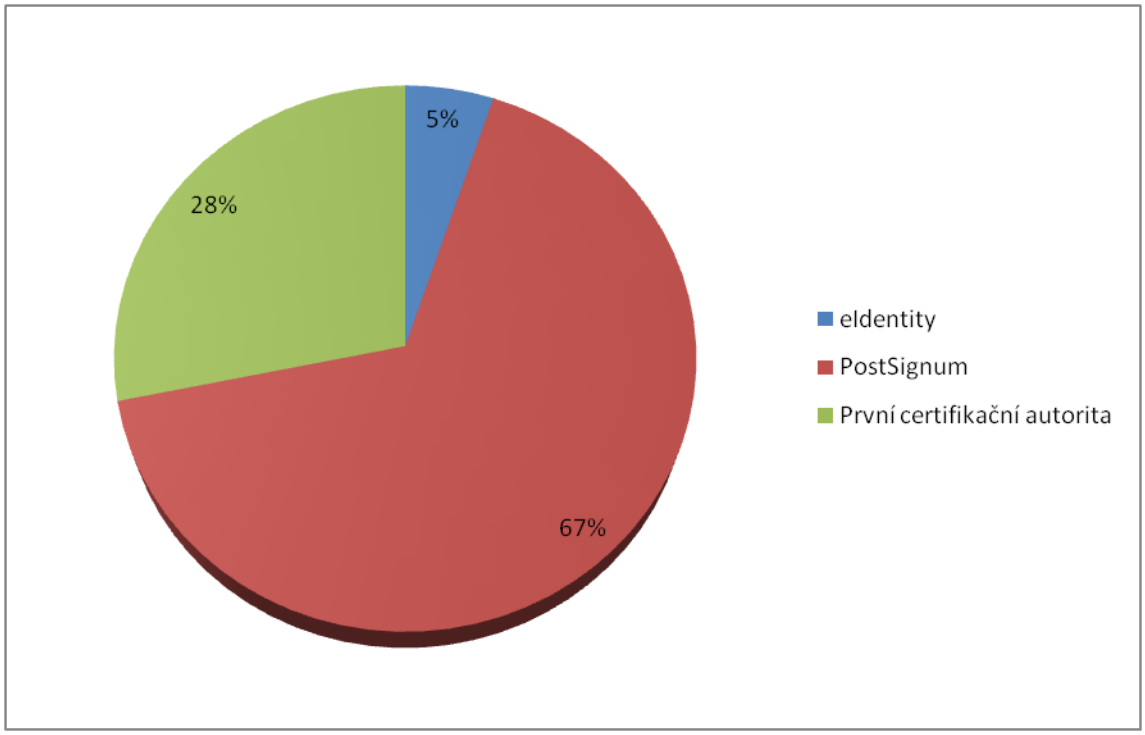
	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Podniky celkem (10+)	**7,0**	**14,0**	**.**	**.**	**20,5**	**21,8**	**23,7**	**48,2**	**59,1**	**65,9**
Velikost podniku										
10–49 zaměstnanců	4,7	9,4	.	.	13,5	14,0	15,6	41,0	53,5	61,2
50–249 zaměstnanců	13,7	26,9	.	.	42,6	46,9	51,2	75,2	78,6	82,9
250 a více zaměstnanců	26,5	48,5	.	.	57,6	66,0	70,7	87,7	90,6	91,4

Zdroj: Šetření o využívání ICT v podnikatelském sektoru (ICT 5-01), ČSÚ 2013

V uvedené tabulce je možné si všimnout od roku 2010 významného nárůstu úplných elektronických podání vůči veřejné správě podniků s více jak 10 zaměstnanci.

Průzkum dále ukázal, že největší podíl certifikátů vydaných kvalifikovaným poskytovatelem certifikačních služeb u respondentů má PostSignum. Využívání certifikátů této autority označilo 66,67 % z celkových 39 respondentů. Je zajímavé, že i společnosti využívající služeb komerčního certifikátu uvedly jednoho z těchto poskytovatelů jako svojí certifikační autoritu.

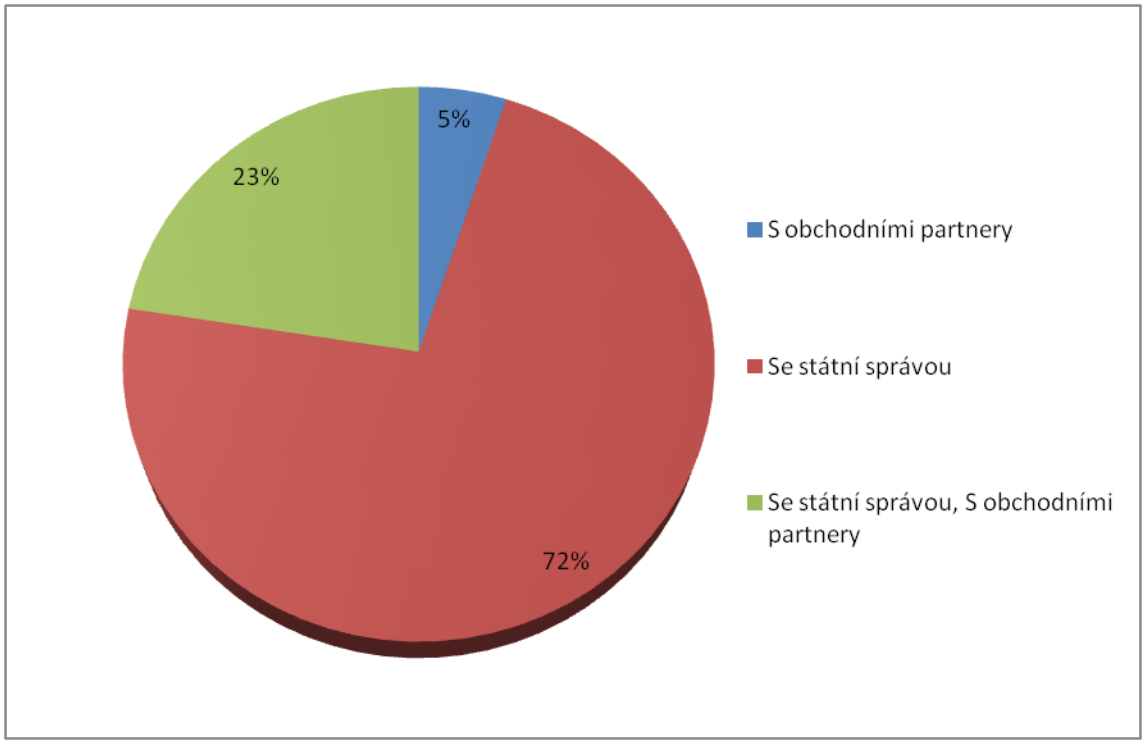
Graf 9 Podíl jednotlivých certifikačních autorit na certifikátech vydaných respondentům



Respondentům byla dále položena otázka ohledně využívání datové schránky v kombinaci s elektronickým podpisem. Z celkového počtu 40 odpovědí 70,45 % odpovědělo kladně. V tomto podílu veškeré společnosti využívají datové schránky při komunikaci s orgány veřejné správy. Nicméně v jedné čtvrtině případů je tato možnost v kombinaci s využitím při komunikací s obchodními partnery. Jedná se především o větší společnosti s 50 – 250 zaměstnanci z činností v oblasti obchodu. Zajímavou skutečností je, že plně důvěřuje zabezpečení tohoto systému pouze 6 z 35 respondentů (17,14 %). Zbylá část se staví k této otázce více skepticky. Přestože největší podíl uvádí, že se doposud nesetkal se žádnými problémy, vyskytly se zde i odpovědi zcela záporné.

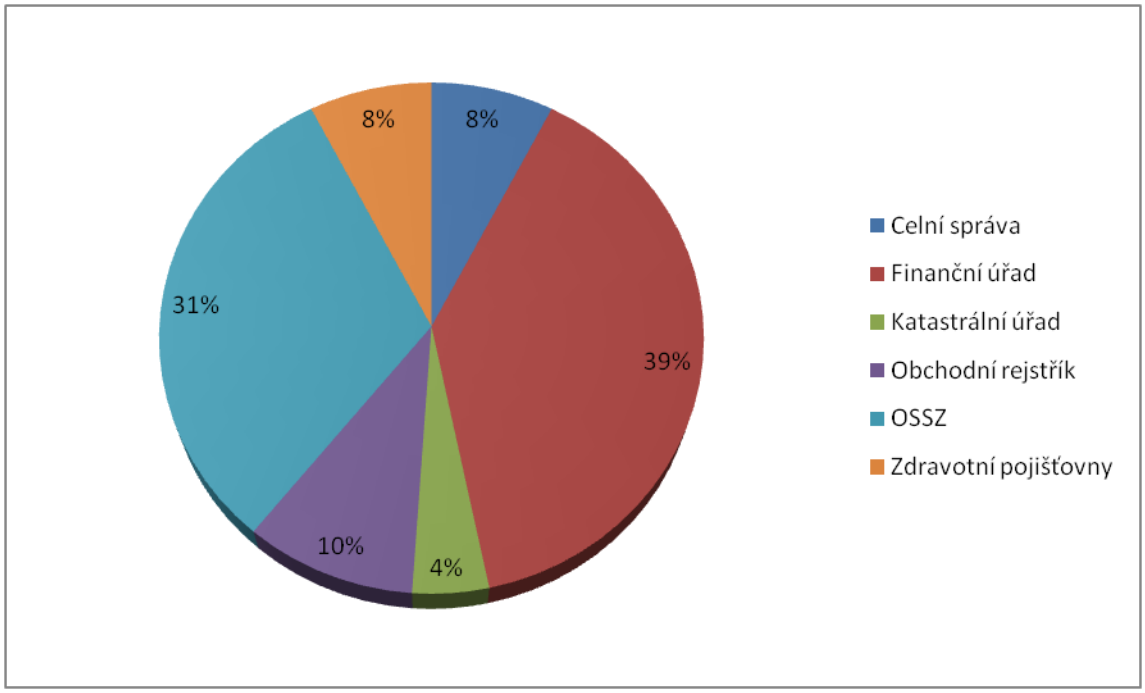
Následující část se již zabývá výsledky průzkumu ohledně využití elektronického podpisu v různých situacích a v různé frekvenci. Pro celkové zhodnocení slouží následující grafy zobrazující podíly z celkových 40 získaných odpovědí.

Graf 10 Využití elektronického podpisu při komunikaci



S jistotou tedy lze říci, že největší podíl využití elektronického podpisu má komunikace s orgány státní správy (95 %). Pouze s obchodními partnery tuto službu využívají dvě firmy ze dvou nejvyšších velikostních kategorií 50 – 250 a více než 250 zaměstnanců. Z důvodu přílišné obecnosti pojmu státní správy byla v rámci dotazníku položena otázka směřující na konkrétní orgány této správy.

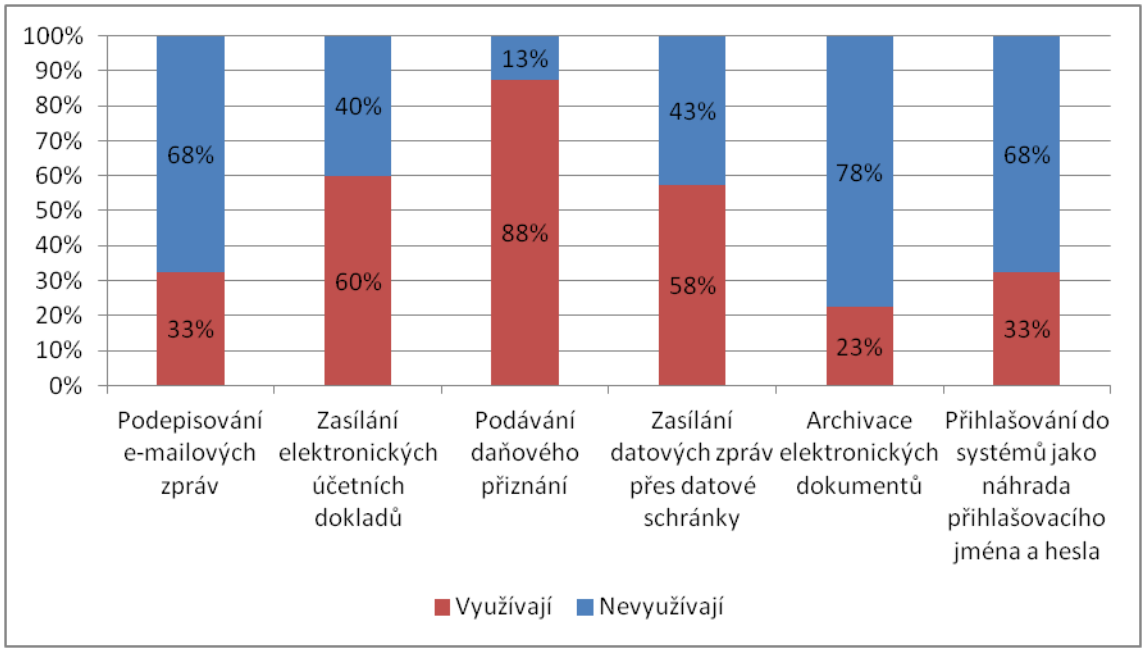
Graf 11 Struktura orgánů veřejné správy, s nimiž společnosti komunikují s použitím elektronického podpisu



V tomto grafu se jedná o podíly na celkových počtech odpovědí. V absolutních hodnotách využívá při komunikaci s finančním úřadem služeb elektronického podpisu 36 společností[61]. Jedna společnost navíc uvedla použití při komunikaci se soudy a jiná s integrovaným systémem plnění ohlašovacích povinností. Podrobnější rozdělení dle kritéria využívání bez zohlednění jeho intenzity je znázorněn dále.

[61] Tento počet koresponduje také s počtem firem uvádějících, že používají elektronický podpis pro podávání daňových přiznání znázorněných v následujícím grafu 12.

Graf 12 Využívání elektronického podpisu v různých oblastech systémů řízení a účetnictví společností



Jak již bylo několikrát prokázáno i zde je možné vidět naprostou převahu využívání elektronického podpisu při podávání daňového přiznání. Ve srovnání s Tabulkou 3 je možné vidět rozdíl v obou průzkumech této kategorie, který je z části způsoben pravděpodobně růstem podniků využívajících možnost podávání daňového přiznání elektronickou formou v roce 2013 a také velikostí výběrového souboru společností, který je u dotazníkového šetření Českého statistického úřadu přibližně 11krát větší.

Nadpoloviční většina respondentů také uvedla, že připojují elektronický podpis k jejich dokumentům v elektronické podobě, jež zasílají třetím stranám přímou cestou (60 %) či prostřednictvím datových schránek (57,5 %). Tento výsledek se značně liší od průzkumu Českého statistického úřadu (ČSÚ), jak je vidět na tabulce níže.

Tabulka 4 Připojování elektronického podpisu k fakturám v elektronické podobě za leden 2013

	Počet podniků celkem[1]	Podniky připojující k el. fakturám elektronický podpis
		podíl na celkovém počtu podniků v dané velikostní a odvětvové skupině (v %)
Podniky celkem (10+)	**39 806**	**8,4**
Velikost podniku		
10–49 zaměstnanců	31 725	6,7
50–249 zaměstnanců	6 603	13,8
250 a více zaměstnanců	1 478	20,5

Zdroj: Šetření o využívání ICT v podnikatelském sektoru (ICT 5-01), ČSÚ 2013

Je diskutabilní, v čem spočívá příčina tohoto nesouladu. Největší vliv má pravděpodobně omezení časového intervalu průzkumu ČSÚ pouze na leden 2013. Dalším možným faktorem je širší pojetí otázky v dotazníku k této diplomové práci, která se ptala na přikládání elektronického podpisu nejen k fakturám ale i dalším elektronickým dokladům. Je nezbytné také zmínit pro potřeby této diplomové práce zahrnutí do průzkumu i podniky s méně než 10 zaměstnanci a osoby samostatně výdělečně činné, avšak kvantitativně menší statistický soubor. Věřím, že tato kritéria společně vytvářejí dostatečně velký rozdíl ve výsledcích pro vysvětlení této odchylky.

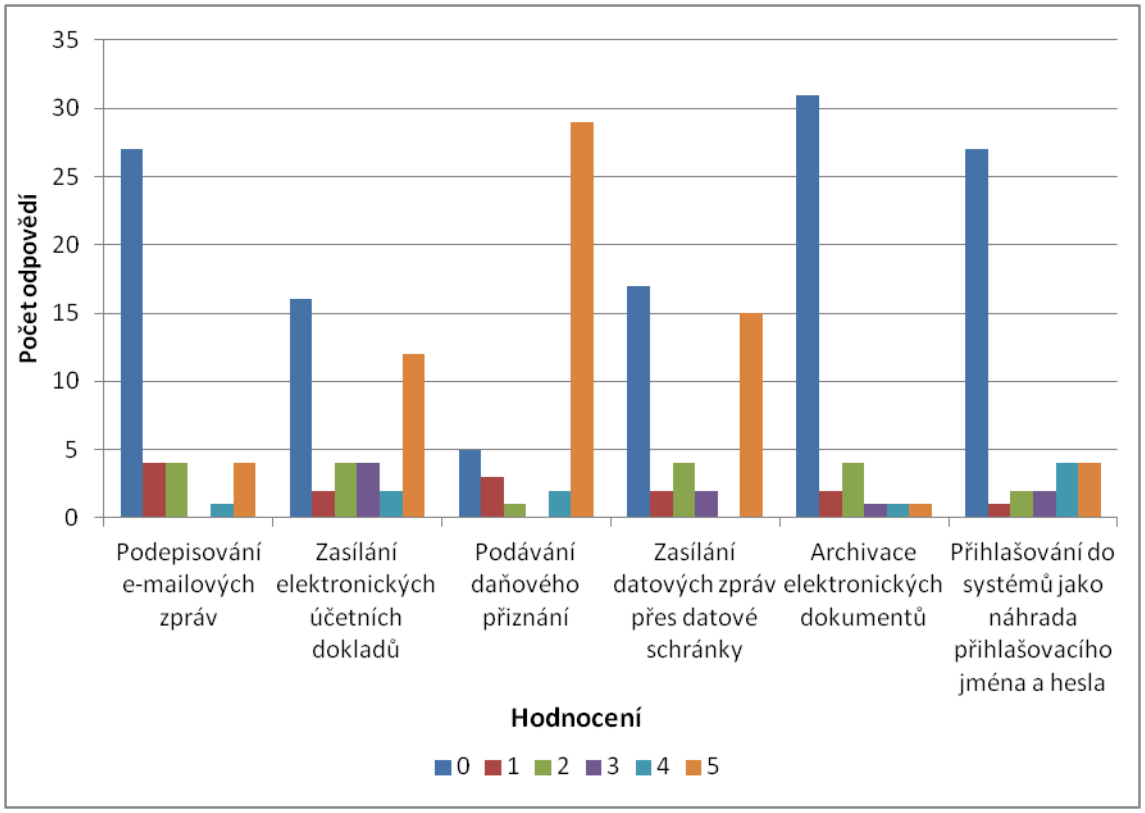
Nejmenší využití v praxi pak elektronický podpis nalézá v kategoriích podepisování emailových zpráv (32,5 %), přihlašování do systémů jako náhrada přihlašovacího jména a hesla (32,5 %) a archivace elektronických dokumentů (22,5 %). Poslední zmiňovaná oblast je nejvíce problematická, jak již bylo dokázáno v teoretické části této diplomové práce. Navíc ze společností archivujících elektronické dokumenty pouze 3 uvedly souběžné využívání kvalifikovaného časového razítka. Dalo by se tedy usoudit, že tyto subjekty jsou jediné, které archivují v elektronické podobě také účetní doklady.

Využívání výhod elektronického podpisu je samozřejmě možné nejen v souvislosti s komunikací třetích stran, ale také uvnitř firmy či holdingu. Bohužel tuto možnost zvolila menšina respondentů. Konkrétně se jedná o pouhých 11 % ze 44 firem využívajících elektronický podpis v různých oblastech podnikání.

Mimo tyto předem vybrané způsoby používání elektronického podpisu byly zaznamenány i jiné odpovědi. Byla zde například zmíněna konverze dokumentů mezi elektronickou a listinou formou, platební styk a hlášení ČSSZ, odesílání přehledů o platbě a přihlášek/odhlášek zdravotním pojišťovnám, využití při výběrových řízeních a samozřejmě také spisová služba.

Pro zhodnocení intenzity využívání elektronického podpisu v různých oblastech podnikání byla tato otázka v dotazníku vyjádřena formou bodování od 0 – 5, kde 0 byla rovna nevyužívání v dané oblasti a 5 nejčastějšímu využití. Výsledky dle uvedené struktury jsou prezentovány v následujícím grafu četností odpovědí.

Graf 13 Hodnocení uživatelů intenzity jejich využívání elektronického podpisu dle jednotlivých oblastí



Společnosti se tedy více méně rozdělují do dvou skupin. Buď elektronický podpis v dané oblasti nevyužívají vůbec, nebo pro každou činnost. Odpovídá to standardnímu postoji maximalizace užitku ze získané služby. Pro lepší porovnání jednotlivých možností mezi sebou jsou dále zobrazena průměrná hodnocení v daných kategoriích.

Tabulka 5 Aritmetický průměr hodnocení intenzity využívání elektronického podpisu v jednotlivých kategoriích

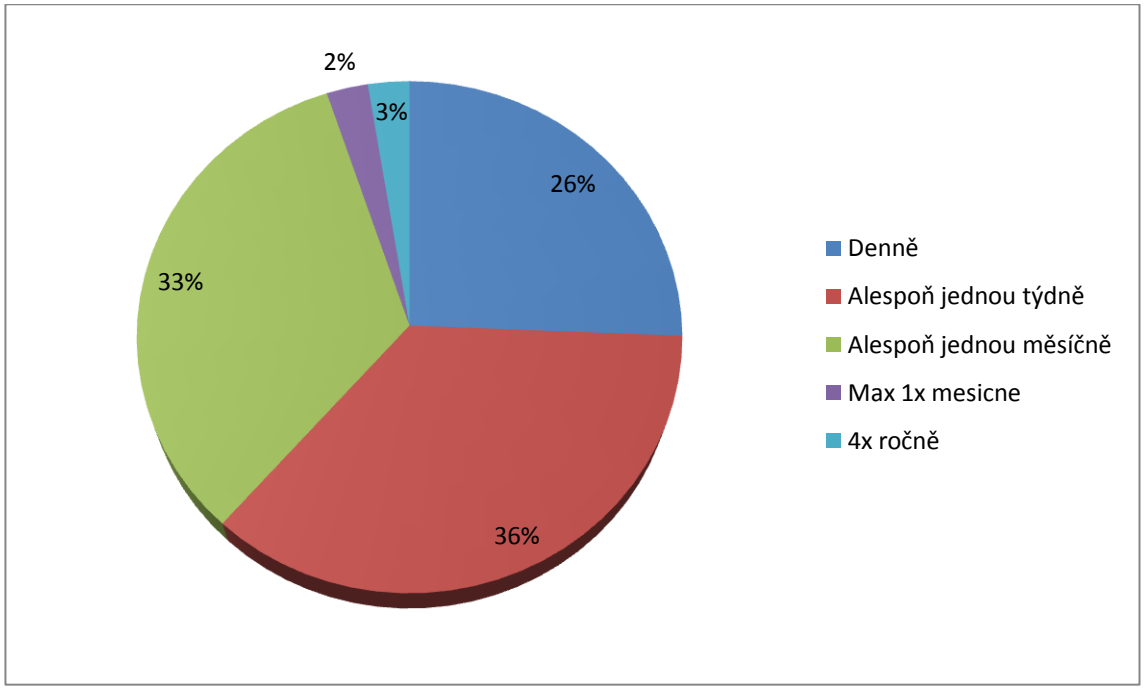
Oblast využívání elektronického podpisu	Průměr
Podepisování e-mailových zpráv	0,90
Zasílání elektronických faktur, dodacích listů a jiných účetních dokladů	2,25
Podávání daňového přiznání	3,95
Zasílání datových zpráv přes datové schránky	2,28
Archivace elektronických dokumentů	0,55
Přihlašování do systémů jako náhrada přihlašovacího jména a hesla	1,18

Z tohoto rozdělení je zřejmé, že pořadí z hlediska nejčastější a nejméně časté oblasti využívání elektronického podpisu se nezměnilo. Avšak po zahrnutí intenzity používání lze vidět, že podepisování emailových zpráv je téměř na stejné úrovni jako archivace elektronických dokumentů. I přesto, že aplikace certifikátu a používání

elektronického podpisu je v oblasti emailové komunikace nejsnáze aplikovatelná. Sporné ovšem zůstává zabezpečování tímto způsobem celou zprávu, pokud její součástí je již jiný dokument s klíčovými informacemi opatřený elektronickým podpisem.

Jelikož však tato stupnice není dle obecně přijímaných měrných jednotek a například podmínky podávání daňových přiznání nebo fakturace jsou individuální pro každý podnikatelský subjekt, byla respondentům položena dodatečná obecná otázka ohledně frekvence využívání elektronického podpisu bez ohledu na situaci, v níž je použit. Výsledkem je poměrně rovnoměrné rozložení.

Graf 14 Frekvence používání elektronického podpisu

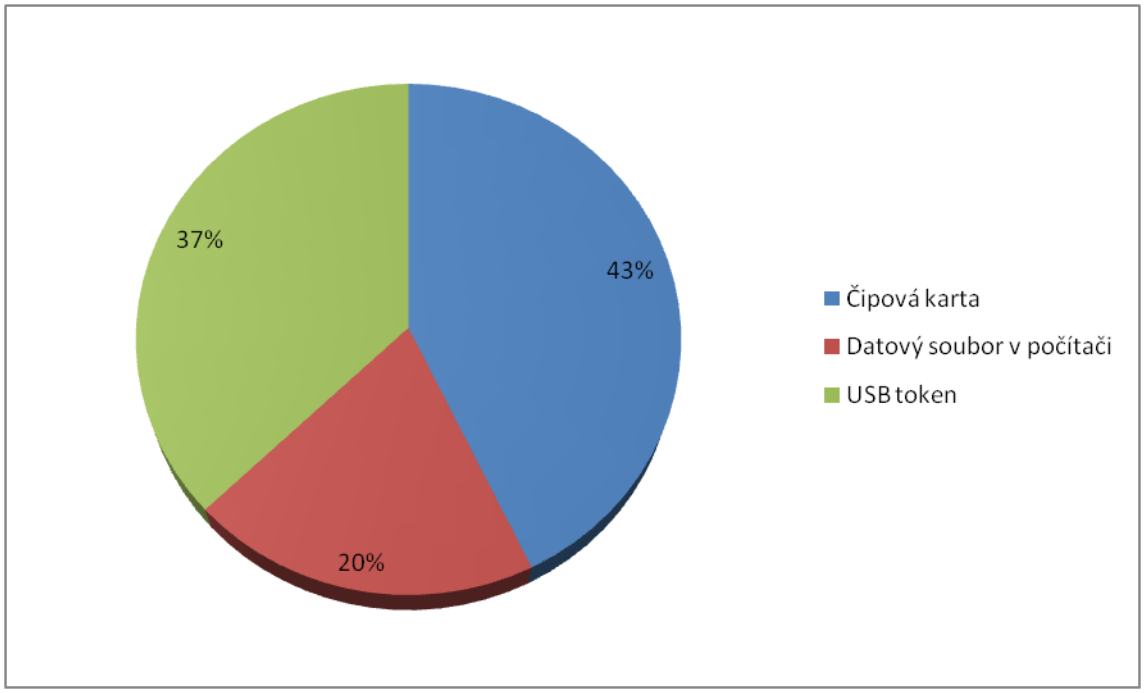


S využíváním na denní bázi je možné se setkat ve 25,64 % případů. Z grafu také vyplývá, že téměř všechny společnosti se zřízeným elektronickým podpisem jej použijí nejméně jednou měsíčně.

Co se týče prostředku pro vytváření elektronických podpisů, velice podobný podíl zastává USB token (37,14 %) a čipová karta (42,86 %). Překvapivá je velice častá odpověď respondentů, kdy ve 20 % případů uchovávají certifikát i soukromý klíč ve formě datového souboru na harddisku počítače. Odpověď na to, zda ochrana počítače jako takového je dostatečná pro minimalizaci rizika zcizení soukromého klíče, se bude pravděpodobně lišit od dané firmy. Nicméně uspokojivý závěr není možné s touto

strukturou otázek dotazníku vydedukovat. Pro lepší představu je uvedeno i grafické znázornění podílů těchto prostředků.

Graf 15 Struktura využívání prostředků pro vytváření elektronických prostředků



Na závěr dotazníku bylo respondentům položeno několik otázek ohledně jejich celkového názoru na silné a slabé stránky elektronického podpisu, případně jaký jeho aspekt by se měl změnit či vylepšit. Účelem bylo zjistit preference uživatelů a doplnění základních podkladů pro hrubou prognózu budoucího vývoje využívání elektronického podpisu v oblasti účetnictví.

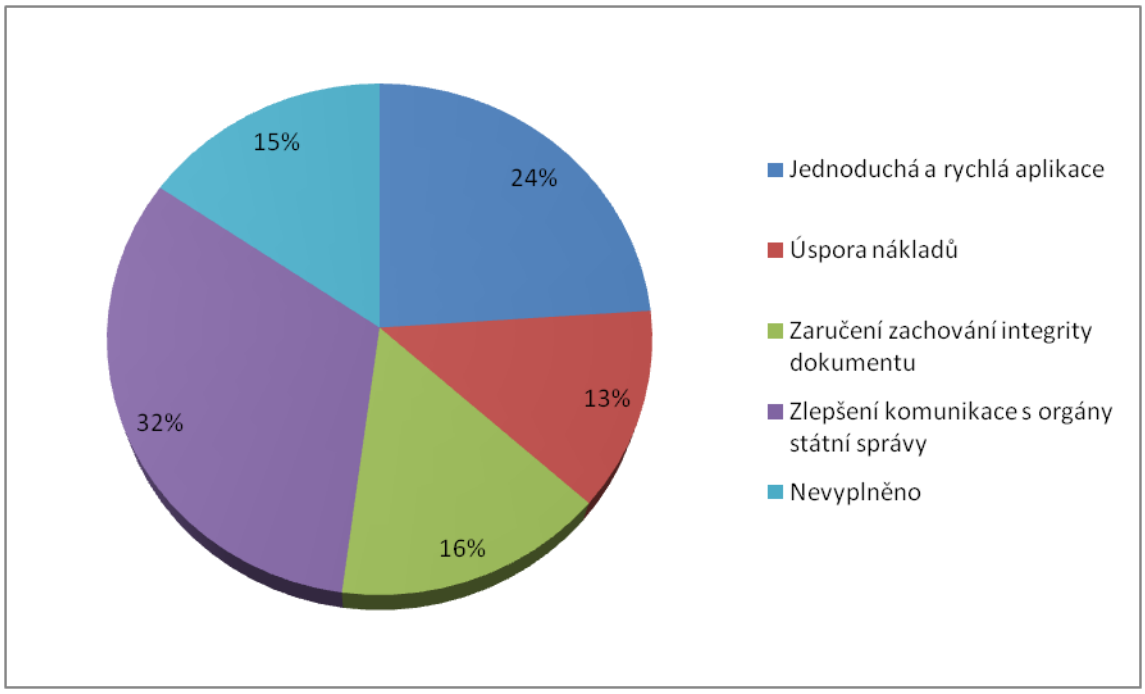
6.3.3 Shrnutí kladů a záporů dle respondentů

Jako největší výhodu vidí 32,39 % společností zlepšení komunikace s orgány státní správy. Jednoduchou a rychlou aplikaci považuje za nejvýraznější přednost 23,94 % dotazovaných. Zaručení zachování integrity dokumentu je reprezentováno v odpovědích na tuto otázku v relativně malé míře (15,49 %). Odpovídá to skutečnosti velice malého využití v rámci interní komunikace podniku a při zasílání elektronických dokumentů. Ovlivňuje to i s vysokou pravděpodobností nedostatečná informovanost veřejnosti o charakteristických znacích elektronického podpisu.[62] Nejmenší počet firem rozpoznává jako největší výhodu úsporu nákladů (12,68 %). Jedná se především o velké firmy s více než 50 zaměstnanci a podniky z oblasti veřejné správy. Tuto možnost

[62] Nedostatečnou informovanost vidí jako hlavní překážku pro využívání elektronického podpisu širší veřejností i jednotlivé 3 firmy. Dokládají to výsledky výzkumu v tabulce 6.

však zvolil jeden podnikatel a dvě společnosti s méně než 10 zaměstnanci nevyužívající elektronický podpis. Přesto jako důvod nevyužívání vidí příliš složitou obnovu certifikátu a náklady s ní spojené.

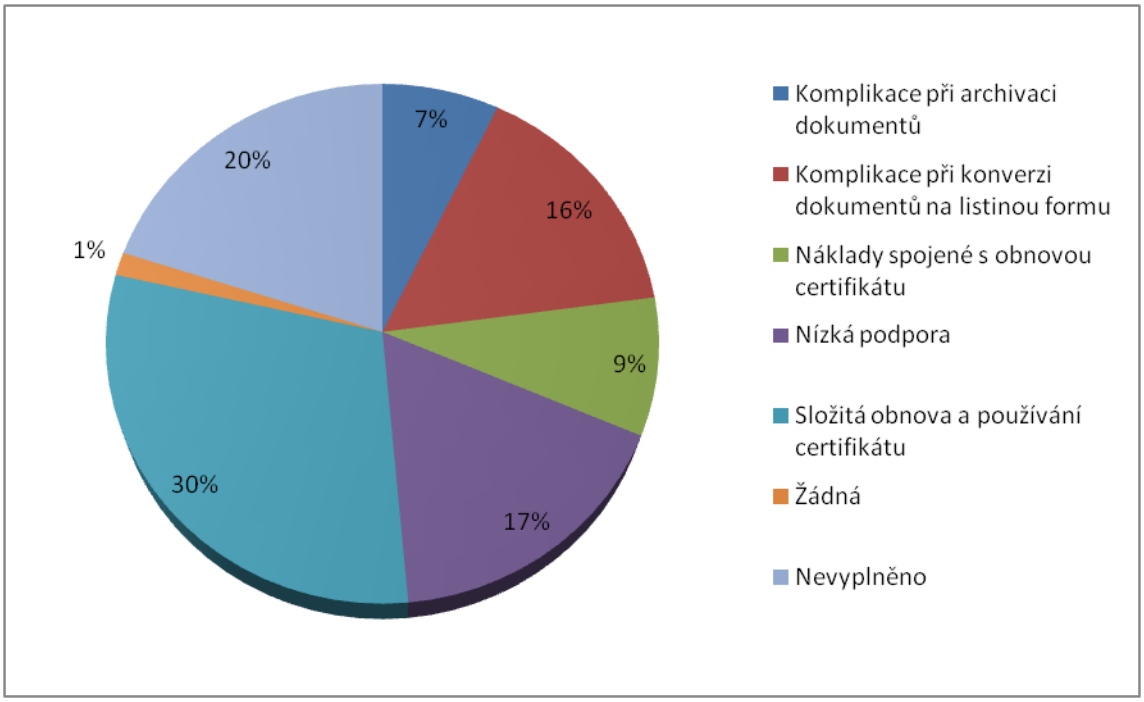
Graf 16 Názor respondentů o největší výhodě elektronického podpisu



Na druhé straně názorů na největší nevýhody elektronického podpisu má největší podíl především složitá obnova a používání certifikátu (30 %). Jako druhá nejčastější odpověď na tuto otázku byly s rozdílem pouze jedné odpovědi od sebe nízká podpora (17,14 %) a komplikace při konverzi dokumentů na listinnou formu (15,71 %).

Jedna osoba samostatně výdělečně činná nevidí v elektronickém podpisu žádnou nevýhodu. Nicméně není vyloučené její setrvání s tímto názorem, jelikož této služby využívá pouze krátce (pořízení v rozmezí let 2010 – 2013) a hlavně při podávání daňových přiznání. Některé slabé stránky na tento podnikatelský subjekt tedy nedopadají v takové míře jako na ostatní společnosti využívající těchto služeb i v ostatních oblastech.

Graf 17 Názor respondentů o největší nevýhodě elektronického podpisu



Z tohoto výčtu byly vypuštěny tři společnosti, které uvedly nedostatek informací jako důvod pro nezodpovězení otázky.

Jako hlavní oblast, na kterou by se mělo Ministerstvo vnitra zaměřit pro budoucí změny je kromě negace zmíněných tří největších slabin elektronického podpisu podle názorů respondentů poskytování certifikátů zdarma nebo přinejmenším jejich zlevnění. Častou odpovědí bylo také zjednodušení všech procesů spojených se zavedením a používáním elektronického podpisu stejně jako zvýšení možností pro jeho využití.

Jako poslední dotaz společnostem využívajícím elektronický podpis byla otázka na jejich názor ohledně oblasti, která nejvíce brání v jeho větším využívání veřejností. Nejvýznamnějším problémem vidí se shodným podílem 38,89 % dotazovaných nedostatek informací a složitý způsob pořízení certifikátu. Jako druhá nejčastější odpověď byly opět se stejným počtem 3 společností činící 8,33 % na všech odpovědích nedostatečná podpora a vyšší pořizovací náklady v poměru k možnostem využití. V následujících datech není uveden názor jedné společnosti, že největší překážkou pro větší rozšíření je obyčejná lenost potenciálních uživatelů. Rozhodně se jedná o zajímavou variantu nabádající k zamyšlení.

Veškeré tyto názory se ukazují jako opodstatněné při porovnání s důvody pro nevyužívání elektronického podpisu u ostatních společností. Jednotlivé oblasti mají

velice podobné podíly na odpovědích za jednotlivé otázky. Na závěr praktické části této diplomové práce jsou na následujících tabulkách tyto kategorie vyznačené u výsledků obou otázek v jednotlivých verzích dotazníku.

Tabulka 6 Názory společností na největší překážku v rozšíření využívání elektronického podpisu

Překážka bránící rozšíření používání	Počet	Podíl
Nedostatečná podpora	3	8,33%
Nedostatek informací	14	38,89%
Složitý způsob pořízení certifikátu	14	38,89%
Vyšší pořizovací náklady v poměru k možnostem využití	3	8,33%
Nedůvěřivost	1	2,78%
Slozite procesy, komplikovanost	1	2,78%
Celkový součet	**36**	**100,00%**

Tabulka 7 Důvody společností, které nemají zřízen elektronický podpis pro jeho nevyužívání

Důvod	Počet	Podíl
Nízká podpora	2	6,67%
Nedostatečné informace pro jeho zřízení	5	16,67%
Složitá obnova a používání certifikátu	6	20,00%
Vysoké náklady na obnovu certifikátu	3	10,00%
Komplikace při archivaci dokumentů	1	3,33%
Komplikace při konverzi dokumentů na listinou formu	2	6,67%
Nevyužitelnost	11	36,67%
Celkem	**30**	**100,00%**

Závěr

Počátky principů elektronického podpisu se datují již od roku 1973, kdy byly vyvinuty základní principy asymetrické kryptografie. Tento pojem se však objevil až v roce 1999 při vydání směrnice Evropské unie. Do naší legislativy byl implementován v roce 2000 zákonem o elektronickém podpisu. Formulace elektronického podpisu tímto právním předpisem byla značně nekompletní a nejasná, a v souvislosti s tím i využití této služby velice omezené. Potřebná aktualizace pro napravení tohoto nedostatku přišla až s novelou daného zákona v roce 2004, jež přinesla nejen upřesnění samotného elektronického podpisu, ale také časových razítek, certifikátů a certifikačních autorit. Od této chvíle neustále narůstá počet uživatelů zmíněných technologií. Právní úprava je samozřejmě nadále upravována. Poslední významnou modifikací byla novela v roce 2012, která řeší mnohé nedostatky ohledně archivace účetních dokladů a komunikace s veřejnou správou.

Elektronický podpis je založený na asymetrické kryptografii, která využívá ve svých algoritmech dvou klíčů – veřejného a privátního. Jejím prostřednictvím je možné zašifrovat jakýkoli datový soubor. Tento proces je však tím časově náročnější, čím více informací je předmětem šifrování. Z toho důvodu se využívá tzv. hashovaní funkce, jež z potřebného souboru vytvoří jedinečný otisk o standardní délce, který se následně zašifruje. Tím vzniká samotný elektronický podpis. Pro jednoznačné určení podepsané osoby je nutné na veřejný klíč každého podpisu vystavit tzv. certifikát. Za tímto účelem byly založeny certifikační autority odpovídající za vydávání, rušení a správu certifikátů.

Jednou z největších výhod elektronického podpisu je především zajištění zachování integrity dokumentu, a pokud je založen na kvalifikovaném certifikátu pak také zabezpečení jednoznačné identifikace podepsané osoby a neodvolatelnosti právního úkonu. Tyto charakteristiky vyplývají z podstaty jeho používání. Další nespornou výhodou je možnost jeho využití při podepsání datového souboru v jakémkoli formátu, či přímo samotného přenosu dat, a zrychlení ověření jeho pravosti a platnosti oproti podpisu vlastnoručnímu.

Naproti tomu mezi největší nedostatky patří především neinformovanost veřejnosti o charakteristických rysech elektronického podpisu. Stále velký podíl osob zaměňuje elektronický podpis za pouhé naskenování vlastnoručního. Rozšíření

používání elektronického podpisu také omezuje složitý proces pořízení certifikátu. Elektronický podpis i hashovací funkce nejsou neprolomitelné, jak se často zobecňuje, ale při současném stupni výpočetních kapacit by překonání jejich algoritmů zabralo příliš mnoho času. V předchozí větě zmíněná skutečnost je výraznou slabinou těchto algoritmů. Adaptací na tento fakt je stanovení omezené platnosti certifikátu. S technologickým pokrokem je tedy nutné vyvíjet neustále nové metody těchto procesů pro zamezení zkrácení doby prolomení na snesitelnou úroveň. Důležité je také zmínit, že nejen elektronický podpis, ale také prostředky pro jeho vytváření mají výraznou slabinu. Jedná se především o mylnou představu nezneužitelnosti čipové karty s privátním klíčem. Vynalézavý hacker však nezaútočí přímo na čipovou kartu, ale na, z hlediska zabezpečení, slabší spojení čtečky karet s počítačem.

Přesto se dá elektronický podpis používat v mnohých situacích, z nichž některé tato práce podrobněji rozebírá. Konkrétně se jedná o využití při elektronické fakturaci, která sice velice často probíhá prostřednictvím zasílání dokumentů emailem, ale je zde i potenciál pro využití v systémech EDI a automatického zpracování dat z konkrétních dokladů. Účetní doklady, jež jsou předmětem této komunikace, musí být archivovány po zákonem stanovený časový interval. Archivace je možná v listinné či elektronické podobě. Avšak archivace elektronických dokumentů zatím nemá vyřešeny veškeré problémy s ní spojené a ani konverze písemností do listinné podoby není bez omezení. Mnohá využití je také možné najít v interním prostředí podniku. Například při podepisování emailů a dokumentů, částečně při automatizaci schvalovacích procesů, při nahrazení přihlašovacího jména a hesla a vytváření sítě VPN. Většina z těchto oblastí má navíc tu výhodu, že nevyžaduje použití kvalifikovaného certifikátu, a společnost si tedy může vytvořit vlastní interní certifikační autoritu pouze pro vlastní potřeby. Dalším a posledním využitím elektronického podpisu, zmíněném v této práci, je jeho úloha v komunikaci se státní správou a samosprávou, a to prostřednictvím datových schránek nebo e-podatelen.

Praktická část byla vypracována formou průzkumu prostřednictvím dotazníkového šetření a jeho analýzy. Ve většině případů se potvrdily teoretické poznatky uvedené v první části této diplomové práce a také mé domněnky.

Ukázalo se, že elektronický podpis využívá nadpoloviční většina respondentů a typově se nejčastěji jedná o zaručený elektronický podpis založený na kvalifikovaném

certifikátu. Jako důvod pro nezřízení elektronického podpisu byla nejčastěji uvedena nevyužitelnost v procesech společností. Relativně významný podíl měl i nedostatek informací pro jeho zřízení a nákladnost a složitost procesu pořízení certifikátu. Poslední zmíněný problém způsobuje i opouštění využívání této služby u ostatních společností. Nicméně zatím se jedná o malé množství firem.

Přes tyto překážky množství společností využívajících elektronický podpis vykazuje dlouhodobý růst s výrazným zvýšením v roce 2010. Dokládá to nejen průzkum této diplomové práce, ale i Českého statistického úřadu. Z výsledku je také zřejmé časté využívání datových schránek v kombinaci s elektronickým podpisem.

Z do této doby získaných poznatků vyplývá nejčastější využití elektronického podpisu, které potvrzují i odpovědi na otázku cílenou na tuto oblast. Nejfrekventovanější uplatnění má především v rámci komunikace s orgány veřejné správy, a to hlavně při podávání úplného elektronického daňového přiznání. Pouze malé procento podnikatelských subjektů využívá těchto služeb jen v rámci styku s obchodními partnery. Jako druhé, z hlediska intenzity využívání elektronického podpisu, bylo uvedeno zasílání elektronických faktur a jiných účetních dokladů a zasílání zpráv přes datové schránky. Oproti tomu nejmenší zastoupení má archivace elektronických dokumentů. Příčinou jsou všechny slabé stránky spojené se správou archiválií v elektronické podobě, rozebrané v teoretické části této práce. Na množství firem archivujících elektronické dokumenty je také závislý počet společností využívajících kvalifikovaná časová razítka.

Překvapující je dle mého názoru rozdělení typů prostředků pro tvorbu elektronického podpisu. Nejvyužívanější variantou je čipová karta, avšak velice častou odpovědí byl certifikát a privátní klíč uložený ve formě datového souboru na harddisku počítače. Nicméně tento způsob je nejméně zabezpečen proti zneužití privátního klíče třetí stranou.

Na závěr praktické části byly analyzovány reakce všech respondentů na otázky ohledně největších kladů a záporů elektronického podpisu a charakteristik, které by se měly změnit pro větší rozšíření jeho používání. Podíly výhod na celkovém počtu odpovědí jsou relativně rovnoměrně rozprostřené. Dvě největší identifikované přednosti byly, jak logicky vyplývá, zlepšení komunikace s orgány státní správy a samosprávy a jednoduchá a rychlá aplikace elektronického podpisu. Největší nevýhodu následně

dotazované společnosti vidí ve složité obnově a používání certifikátů. Významný podíl mají však i komplikace při konverzi dokumentů na listinnou formu a obecně nízká podpora.

Poslední položenou otázkou pro společnosti využívající elektronický podpis bylo vyjádření jejich názoru ohledně největší překážky pro větší rozšíření používání této služby. Výsledky byly porovnány s důvody firem pro jeho nevyužívání. Z těchto odpovědí jsou čtyři z nich obdobně formulované a byly zaznamenané při analýze výsledků obou otázek. V následujícím seznamu jsou seřazené sestupně dle jejich podílu na celkovém počtu odpovědí:

- složitý způsob pořízení certifikátu,
- nedostatek informací,
- vyšší pořizovací náklady v poměru k možnostem využití,
- nedostatečná podpora.

Elektronický podpis má potenciál na urychlení administrativních procesů nejen v rámci podnikatelské činnosti, ale také v životě soukromých osob. Na tomto místě bych však chtěl vyzdvihnout problém, který považuji za největší překážku pro jeho rozšíření. Je jím *nedostatek informací*. Soukromé osoby ve většině případů neví, co to elektronický podpis je, jaké má výhody a nevýhody, ani kde je možné jej použít. Otázkou však zůstává, kdo by měl mít zodpovědnost za rozšíření těchto informací. Dle mého názoru, nejlepším řešením by bylo zavedení jeho podrobného rozboru do výuky informačních technologií již na středních školách. Domnívám se, že pokud by se vyřešil tento problém, mnoho dalších by se stalo irelevantní. Zvýšilo by se tím množství společností využívajících elektronický podpis, a tím by došlo i ke zvýšení způsobů využití této služby. Nevyužitelnost by tak přestala být překážkou. To by vedlo k větší poptávce po certifikátech a mohlo zapříčinit vznik dalších kvalifikovaných certifikačních autorit. Nárůst konkurence by následně tlačil na snižování cen, a tím by se pravděpodobně vyřešily problémy s vysokými počátečními náklady v porovnání s přínosy.

Nic z výše uvedeného však není možné bez dostatečné vládní podpory prostřednictvím zákonů a další propagace plně elektronické komunikace s orgány veřejné správy. Přesto si myslím, že budoucí vývoj bude příznivý zejména v oblasti soukromého využívání elektronického podpisu a při zasílání faktur a jiných účetních

dokladů. Tento závěr podporují i výsledky dotazníku, kde většina společností nevyužívajících této služby by si ji pořídila právě za účelem zasílání elektronických dokumentů.

Zdroje

Odborná literatura

[1] BUDIŠ, Petr. *Elektronický podpis a jeho aplikace v praxi*. 1. vyd. Olomouc: ANAG, 2008. 157 s. Právo. ISBN 978-80-7263-465-1.

[2] MEJZLÍK, Ladislav. *Účetní informační systémy: využití informačních a komunikačních technologií v účetnictví*. Vyd. 1. Praha: Oeconomica, 2006. 173 s. ISBN 80-245-1136-3.

[3] PETERKA, Jiří. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, ©2011. 430 s. CZ.NIC. ISBN 978-80-904248-3-8.

[4] SMEJKAL, Vladimír a VALÁŠEK, Michal Altair. *Jak na datové schránky: praktický manuál pro každého*. Praha: Linde Praha, 2012. 197 s. ISBN 978-80-86131-80-1.

[5] ŠTĚDROŇ, Bohumír. *Manažerské řízení a informační technologie*. 1. vyd. Praha: Grada, 2007. 156 s. ISBN 978-80-247-2052-4.

Zdroje pro praktickou část

[6] Oficiální webový portál Zlatých stránek [cit. 2014-05-10]. Dostupné z:http://www.zlatestranky.cz/

[7] Průzkumy podnikatelského sektoru provedené Českým statistickým úřadem [cit. 2014-05-11]. Dostupné z: http://www.czso.cz/csu/redakce.nsf/i/podnikatelsky_sektor

Právní předpisy

[8] Rozhodnutí Komise 2009/767/ES ze dne 16. října 2009, kterým se stanovují opatření pro usnadnění užití postupů s využitím elektronických prostředků prostřednictvím „jednotných kontaktních míst“ podle směrnice Evropského parlamentu a Rady 2006/123/ES o službách na vnitřním trhu

[9] Rozhodnutí Komise 2011/130/EU ze dne 25. února 2011, kterým se stanoví minimální požadavky na příhraniční zpracování dokumentů elektronicky podepsaných příslušnými orgány podle směrnice 2006/123/ES Evropského parlamentu a Rady o službách na vnitřním trhu

[10] Směrnice 1999/93/EC Evropského parlamentu a Rady ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy

[11] Vyhláška č. 212/2012 Sb., o struktuře údajů, na základě kterých je možné jednoznačně identifikovat podepisující osobu, a postupech pro ověřování platnosti zaručeného elektronického podpisu, elektronické značky, kvalifikovaného certifikátu, kvalifikovaného systémového certifikátu a kvalifikovaného časového razítka

[12] Vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb, o požadavcích na nástroje elektronického podpisu a o požadavcích na ochranu dat pro vytváření elektronických značek

[13] Vyhláška č. 496/2004 Sb., o elektronických podatelnách

[14] Zákon č. 2/1969 Sb., o zřízení ministerstev a jiných ústř. orgánů státní správy ČR ve znění pozdějších předpisů

[15] Zákon č. 227/2000 Sb., o elektronickém podpisu ve znění pozdějších předpisů

[16] Zákon č. 280/2009 Sb., daňový řád ve znění pozdějších předpisů

[17] Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů ve znění pozdějších předpisů

[18] Zákon č. 499/2004 Sb., o archivnictví a spisové službě ve znění pozdějších předpisů

[19] Zákon č. 563/1991 Sb., o účetnictví ve znění pozdějších předpisů

Ostatní zdroje

[20] ČERMÁK, Miroslav. *Základy kryptografie pro manažery: certifikační autorita* [online]. 15. 5. 2011 [cit. 2014-05-11]. Dostupné z:http://www.cleverandsmart.cz/zaklady-kryptografie-pro-manazery-certifikacni-autorita/

[21] *DLOUHODOBÁ ARCHIVACE ELEKTRONICKÝCH ORIGINÁLŮ DOKUMENTŮ: Jak zajistit čitelnost a nezpochybnitelnost dokumentů po neomezeně dlouhou dobu* [online]. [cit. 2014-05-02]. Dostupné z: https://www.602.cz/files/Svet602_2012_web.pdf?sid=3290

[22] *Elektronická podání pro finanční správu* [online]. 1. 1. 2013 [cit. 2014-05-15]. Dostupné z: http://www.financnisprava.cz/cs/dane-elektronicky/danovy-portal/elektronicka-podani-pro-financni-spravu

[23] *Elektronické podání a DIS, změna daňového řádu* [online]. 20. 12. 2013 [cit. 2014-04-26]. Dostupné z:http://adisspr.mfcr.cz/adistc/adis/idpr_pub/dpr_info/aktualita.faces?zaznam=46

[24] LEVEY, Lewis D. *B2C Electronic Signatures: Building Stronger Consumer Relationships* [online]. [cit. 2014-04-15]. Dostupné z:http://c.ymcdn.com/sites/www.bfma.org/resource/resmgr/Articles/08_43.pdf?hhSearchTerms=%22building+and+stronger+and+consumer+and+relationships%22

[25] NÁPRAVNÍK, Jiří. *Časovaná bomba jménem (ne)zaručený elektronický podpis* [online]. 14. 6. 2013 [cit. 2014-05-16]. Dostupné z:http://www.root.cz/clanky/casovana-bomba-jmenem-ne-zaruceny-elektronicky-podpis/

[26] NÁPRAVNÍK, Jiří. *Jsou čipové karty bezpečné?* [online]. 27. 3. 2006 [cit. 2014-05-16]. Dostupné z: http://www.lupa.cz/clanky/jsou-cipove-karty-bezpecne/

[27] NÁPRAVNÍK, Jiří. *Vše o zaručeně zneužitelném elektronickém podpisu* [online]. 22. 3. 2013 [cit. 2014-05-08]. Dostupné z:http://napravnik.blog.ihned.cz/c1-59489550-vse-o-zarucene-zneuzitelnem-elektronickem-podpisu

[28] NÁPRAVNÍK, Jiří. *Zaručený elektronický podpis má bezpečnostní mezery* [online]. 9. 9. 2013 [cit. 2014-05-01]. Dostupné z:http://www.mesec.cz/clanky/zaruceny-elektronicky-podpis-ma-bezpecnostni-mezery/

[29] *Novela rozhodnutí Komise 2009/767/ES* [online]. 30. 11. 2010 [cit. 2014-05-05]. Dostupné z:http://www.mvcr.cz/clanek/novela-rozhodnuti-komise-2009-767-es.aspx

[30] Oficiální webový portál ePodatelny Ministerstva spravedlnosti České republiky. Dostupné z: http://epodatelna.justice.cz/ePodatelna/epo1200new/form.do

[31] Oficiální webový portál formátu ISDOC [cit. 2014-05-06]. Dostupné z: http://www.isdoc.cz/

[32] Oficiální webový portál ICT Unie [cit. 2014-05-06]. Dostupné z: http://www.ictu.cz/

[33] Oficiální webový portál Ministerstva vnitra České republiky. Dostupné z: http://www.mvcr.cz/clanek/informace-k-pouzivani-elektronickeho-podpisu.aspx

[34] Oficiální webový portál První certifikační autority. Dostupné z: http://www.ica.cz/

[35] Oficiální webový portál Vlády České republiky [cit. 2014-05-11]. Dostupné z: http://www.vlada.cz/

[36] PDF/A. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 18. 2. 2014 [cit. 2014-05-03]. Dostupné z:http://cs.wikipedia.org/wiki/PDF/A

[37] PETERKA, Jiří. *Elektronický podpis* [online]. [cit. 2014-04-20]. Dostupné z: http://www.earchiv.cz/i_digsig.php3

[38] PETERKA, Jiří. *Co je elektronický podpis?* [online]. 4. 5. 2000 [cit. 2014-04-19]. Dostupné z:http://www.earchiv.cz/b00/b0405001.php3

[39] PETERKA, Jiří. *Česká cesta k elektronickému podpisu?* [online]. 06/2000 [cit. 2014-04-21]. Dostupné z:http://www.earchiv.cz/b00/b0006001.php3

[40] PETERKA, Jiří. *Jak budou fungovat elektronické podpisy po 1. červenci?* [online]. 25. 6. 2012 [cit. 2014-05-02]. Dostupné z:http://www.earchiv.cz/b12/b0625001.php3

[41] PETERKA, Jiří. *Názvoslovné omyly světa počítačů* [online]. 17. 2. 2000, III. [cit. 2014-05-09]. Dostupné z:http://www.earchiv.cz/anovinky/ai3731.php3

[42] PETERKA, Jiří. *Parazitům (OSVČ) povinně datovou schránku nebo elektronický podpis!* [online]. 18. 3. 2013 [cit. 2014-05-12]. Dostupné z:http://www.mesec.cz/clanky/osvc-povinne-datove-schranky-nebo-elektronicky-podpis/

[43] PETERKA, Jiří. *Proč elektronické podpisy nejsou věčné?* [online]. 10. 5. 2010 [cit. 2014-04-29]. Dostupné z:http://www.earchiv.cz/b10/b0510001.php3

[44] PETERKA, Jiří. *Stalo se: elektronický podpis prý platí, dokud se neprokáže opak* [online]. 14. 9. 2009 [cit. 2014-05-09]. Dostupné z: http://www.earchiv.cz/b09/b0914001.php3

[45] REICHEL, David. *Jak na elektronickou výměnu dat?* [online]. 09/2009 [cit. 2014-05-15]. Dostupné z: http://data.businessworld.cz/file/elektronicka-vymena-dat.pdf

[46] ŠTĚDROŇ, Bohumír. SINGULAR CZECH, s.r.o. *Obchodování na internetu, bankovní služby, elektronická certifikace, digitální podpisy a další nové trendy ICT* [online]. Praha, 2007 [cit. 2014-04-30]. Dostupné z: http://www.mmr.cz/getmedia/43f54c4d-454d-48b9-a4c0-2f1369d841a5/GetFile8_2.pdf

[47] *The "Red October" Campaign: An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies* [online]. 14. 1. 2014 [cit. 2014-05-16]. Dostupné z: http://www.root.cz/clanky/casovana-bomba-jmenem-ne-zaruceny-elektronicky-podpis/

[48] VONDRUŠKA, Pavel. *Cesta kryptografie do nového tisíciletí: Od Kámasutry k osobním zápiskum K. H. Máchy*. ComputerWorld 37/2000–40/2000

[49] *Vznik ICT UNIE* [online]. 29. 1. 2010 [cit. 2014-05-08]. Dostupné z:http://www.itbiz.cz/vznik-ict-unie

Přílohy

Seznam obrázků

OBRÁZEK 1 PROCES PODEPSÁNÍ A PŘENOSU DATOVÉ ZPRÁVY 10
OBRÁZEK 2 PŘÍKLAD OTISKŮ JEDNODUCHÉHO TEXTU 11
OBRÁZEK 3 PROCES PODEPSÁNÍ A ODESLÁNÍ ZPRÁVY A JEJÍ OVĚŘENÍ ADRESÁTEM 12
OBRÁZEK 4 BEZPEČNÁ KOMUNIKACE S VYUŽITÍM ELEKTRONICKÉHO PODPISU 13
OBRÁZEK 5 VÝŇATEK Z CERTIFIKÁTU V TEXTOVÉM SOUBORU 16
OBRÁZEK 6 HASH KOŘENOVÉHO CERTIFIKÁTU PRVNÍ CERTIFIKAČNÍ AUTORITY DLE OFICIÁLNÍHO WEBOVÉHO PORTÁLU 17
OBRÁZEK 7 HASH KOŘENOVÉHO CERTIFIKÁTU PRVNÍ CERTIFIKAČNÍ AUTORITY DLE MINISTERSTVA VNITRA ČESKÉ REPUBLIKY 18
OBRÁZEK 8 SEZNAM KVALIFIKOVANÝCH CERTIFIKAČNÍCH AUTORIT 20
OBRÁZEK 9 SEZNAM AKREDITOVANÝCH CERTIFIKAČNÍCH AUTORIT 21
OBRÁZEK 10 PRVNÍ PRINCIP AUTORIZACE KLIENTA PŘI PŘIHLAŠOVÁNÍ DO INFORMAČNÍHO SYSTÉMU 36
OBRÁZEK 11 DRUHÝ PRINCIP AUTORIZACE KLIENTA PŘI PŘIHLAŠOVÁNÍ DO INFORMAČNÍHO SYSTÉMU 37
OBRÁZEK 12 PODÍL PODNIKŮ VYUŽÍVAJÍCÍCH ELEKTRONICKÝ PODPIS A DATOVÉ SCHRÁNKY PŘI KOMUNIKACI S VEŘEJNOU SPRÁVOU ZA ROK 2012 40

Seznam tabulek

TABULKA 1 VYBRANÉ SPOLEČNOSTI ČINNÉ VE VÍCE OBORECH PODNIKÁNÍ 49
TABULKA 2 DETAIL SPECIFICKÝCH ODPOVĚDÍ RESPONDENTŮ Z OBLASTI OBCHODU, KTEŘÍ UVAŽUJÍ O POŘÍZENÍ EP 51
TABULKA 3 PODNIKY POUŽÍVAJÍCÍ INTERNET K ÚPLNÉMU ELEKTRONICKÉMU PODÁNÍ URČENÉHO PRO VEŘEJNOU SPRÁVU 55
TABULKA 4 PŘIPOJOVÁNÍ ELEKTRONICKÉHO PODPISU K FAKTURÁM V ELEKTRONICKÉ PODOBĚ ZA LEDEN 2013 59
TABULKA 5 ARITMETICKÝ PRŮMĚR HODNOCENÍ INTENZITY VYUŽÍVÁNÍ ELEKTRONICKÉHO PODPISU V JEDNOTLIVÝCH KATEGORIÍCH 61

TABULKA 6 NÁZORY SPOLEČNOSTÍ NA NEJVĚTŠÍ PŘEKÁŽKU V ROZŠÍŘENÍ VYUŽÍVÁNÍ ELEKTRONICKÉHO PODPISU 66
TABULKA 7 DŮVODY SPOLEČNOSTÍ, KTERÉ NEMAJÍ ZŘÍZEN ELEKTRONICKÝ PODPIS PRO JEHO NEVYUŽÍVÁNÍ 66

Seznam grafů

GRAF 1 STRUKTURA ODPOVĚDÍ DLE UMÍSTĚNÍ SÍDLA SPOLEČNOSTI RESPONDENTŮ 47
GRAF 2 STRUKTURA ODPOVĚDÍ DLE PRÁVNÍ FORMY RESPONDENTŮ 48
GRAF 3 STRUKTURA ODPOVĚDÍ DLE PŘEDMĚTU PODNIKÁNÍ A VELIKOSTI SPOLEČNOSTÍ .. 49
GRAF 4 VYUŽITÍ ELEKTRONICKÉHO PODPISU DLE JEJICH DRUHŮ 50
GRAF 5 PLÁNY SPOLEČNOSTÍ OHLEDNĚ POŘÍZENÍ ELEKTRONICKÉHO PODPISU V BUDOUCNU STRUKTUROVANÉ DLE PŘEDMĚTU PODNIKÁNÍ 51
GRAF 6 DŮVODY RESPONDENTŮ PRO NEVYUŽÍVÁNÍ EP V SOUČASNOSTI 52
GRAF 7 OBLAST VYUŽITÍ ELEKTRONICKÉHO PODPISU ZAKLÁDAJÍCÍ DŮVOD PRO JEHO POŘÍZENÍ BEZ OHLEDU NA SKUTEČNÝ ZÁMĚR SPOLEČNOSTÍ O JEHO BUDOUCÍM VYUŽÍVÁNÍ 53
GRAF 8 OBDOBÍ POČÁTKU VYUŽÍVÁNÍ ELEKTRONICKÉHO PODPISU 54
GRAF 9 PODÍL JEDNOTLIVÝCH CERTIFIKAČNÍCH AUTORIT NA CERTIFIKÁTECH VYDANÝCH RESPONDENTŮM 56
GRAF 10 VYUŽITÍ ELEKTRONICKÉHO PODPISU PŘI KOMUNIKACI 57
GRAF 11 STRUKTURA ORGÁNŮ VEŘEJNÉ SPRÁVY, S NIMIŽ SPOLEČNOSTI KOMUNIKUJÍ S POUŽITÍM ELEKTRONICKÉHO PODPISU 58
GRAF 12 VYUŽÍVÁNÍ ELEKTRONICKÉHO PODPISU V RŮZNÝCH OBLASTECH SYSTÉMŮ ŘÍZENÍ A ÚČETNICTVÍ SPOLEČNOSTÍ 59
GRAF 13 HODNOCENÍ UŽIVATELŮ INTENZITY JEJICH VYUŽÍVÁNÍ ELEKTRONICKÉHO PODPISU DLE JEDNOTLIVÝCH OBLASTÍ 61
GRAF 14 FREKVENCE POUŽÍVÁNÍ ELEKTRONICKÉHO PODPISU 62
GRAF 15 STRUKTURA VYUŽÍVÁNÍ PROSTŘEDKŮ PRO VYTVÁŘENÍ ELEKTRONICKÝCH PROSTŘEDKŮ 63
GRAF 16 NÁZOR RESPONDENTŮ O NEJVĚTŠÍ VÝHODĚ ELEKTRONICKÉHO PODPISU 64
GRAF 17 NÁZOR RESPONDENTŮ O NEJVĚTŠÍ NEVÝHODĚ ELEKTRONICKÉHO PODPISU 65

Dotazník k diplomové práci: Elektronický podpis a jeho využití v účetnictví

Legenda:

Elektronický podpis = podpis pouze fyzické osoby
Elektronická značka = prostřednictvím značky se mohou podepisovat i společnosti jako celek

"Rozdíl mezi zaručeným a klasickým elektronickým podpisem je stejný jako u ověřeného a neověřeného ručního podpisu." - Zaručený elektronický podpis datové zprávy; 5.6.2010; http://www.datoveschranky.eu/

*Povinné pole

Společné otázky

1. Jaká je právní forma Vaší společnosti? *

Označte jen jednu elipsu.

- ◯ Veřejná obchodní společnost
- ◯ Komanditní společnost
- ◯ Společnost s ručením omezeným
- ◯ Akciová společnost
- ◯ OSVČ
- ◯ Státní podnik
- ◯ Družstvo

2. Jaký je hlavní předmět činnosti Vašeho podnikání? *

Zaškrtněte všechny platné možnosti.

- ☐ Výroba
- ☐ Obchod
- ☐ Finanční služby
- ☐ Poradenské služby
- ☐ Ostatní služby
- ☐ Informační technologie, výzkum a vývoj
- ☐ Státní a veřejná správa
- ☐ Vzdělávání a školství

3. Jaký je počet Vašich zaměstnanců? *

Označte jen jednu elipsu.

- ◯ méně než 10
- ◯ 10 - 49
- ◯ 50 - 250
- ◯ více než 250

4. V jakém kraji má Vaše firma sídlo? *

Označte jen jednu elipsu.

- ◯ Hlavní město Praha
- ◯ Středočeský
- ◯ Jihočeský
- ◯ Plzeňský
- ◯ Karlovarský
- ◯ Ústecký
- ◯ Liberecký
- ◯ Královéhradecký
- ◯ Pardubický
- ◯ Vysočina
- ◯ Jihomoravský
- ◯ Olomoucký
- ◯ Moravskoslezský
- ◯ Zlínský

5. Využíváte elektronický podpis a pokud ano tak jaký? *

Zvolte možnost jež používáte nejčastěji

Označte jen jednu elipsu.

- ◯ Elektronický podpis
- ◯ Zaručený elektronický podpis založený na kvalifikovaném certifikátu
- ◯ Elektronická značka
- ◯ Elektronická značka založená na kvalifikovaném certifikátu
- ◯ Nevyužíváme

Verze pro respondenty nevyužívající elektronický podpis

6. Uvažujete o používání elektornického podpisu v budoucnu?

Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

7. Pokud byste uvažovali o pořízení elektronického podpisu, tak za jakým účelem?

Zaškrtněte všechny platné možnosti.

- ☐ Podepisování emailových zpráv
- ☐ Zasílání elektronických faktur, dodacích listů a jiných účetních dokladů
- ☐ Podávání daňového přiznání
- ☐ Zasílání datových zpráv přes datové schránky
- ☐ Archivace elektronických dokumentů
- ☐ Přihlašování do systémů jako náhrada přihlašovacího jména a hesla
- ☐ Jiné: _____

8. Jaká je dle Vašeho mínění největší výhoda elektronického podpisu?

Označte jen jednu elipsu.

- ◯ Úspora nákladů
- ◯ Jednoduchá a rychlá aplikace
- ◯ Zaručení zachování integrity dokumentu
- ◯ Zlepšení komunikace s orgány státní správy
- ◯ Jiné: _____

9. Jaká je dle Vašeho mínění největší nevýhoda elektronického podpisu?

Označte jen jednu elipsu.

- ◯ Komplikace při archivaci dokumentů
- ◯ Komplikace při konverzi dokumentů na listinou formu
- ◯ Náklady spojené s obnovou certifikátu
- ◯ Složitá obnova a používání certifikátu
- ◯ Nízká podpora
- ◯ Jiné: _____

10. Z jakého důvodu nevyužíváte elektronický podpis?

Zaškrtněte všechny platné možnosti.

- [ ] Vysoké náklady na obnovu certifikátu
- [ ] Nevyužitelnost
- [ ] Nedostatečné informace pro jeho zřízení
- [ ] Nevýhoda uvedená v předchozí otázce
- [ ] Jiné: _____

11. Jaký je Váš názor na výši ročních nákladů na obnovu certifikátu?

Označte jen jednu elipsu.

- ◯ Příliš vysoké
- ◯ Nadprůměrné
- ◯ Přiměřené
- ◯ Nízké
- ◯ Neznám jejich přesnou výši

12. Co by se dle Vašeho názoru mělo na elektronickém podpisu změnit či vylepšit?

_____

Verze pro respondenty využívající elektronický podpis

Na této stránce prosím odpovídejte z hlediska nejčastěji využívané podoby elektronického podpisu, kterou jste uvedli v 5. otázce.

6. Uvažujete o využívání elektronického podpisu i v budoucnu?

Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

7. Využíváte společně s elektronickým podpisem i kvalifikované časové razítko?

Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne

8. U jaké certifikační autority máte zřízen elektronický podpis?

Označte jen jednu elipsu.

- ◯ První certifikační autorita
- ◯ eIdentity
- ◯ PostSignum
- ◯ Jiné: _____

9. Od jakého roku používáte elektronický podpis?

Označte jen jednu elipsu.

- 2000 - 2001
- 2002 - 2003
- 2004 - 2006
- 2007 - 2009
- 2010 - 2013

10. V rámci jakého styku elektronický podpis využíváte?

Zaškrtněte všechny platné možnosti.

- [ ] Interní komunikace v podniku
- [ ] Komunikace v rámci holdingu
- [ ] Se státní správou
- [ ] S obchodními partnery
- [ ] Jiné: _____

11. Využíváte datové schránky?

Označte jen jednu elipsu.

- Ano
- Ne

12. Využíváte datové schránky pouze pro komunikaci s orgány státní správy či i s obchodními partnery?

Označte jen jednu elipsu.

- Pouze s orgány státní správy
- Se státní správou i s obchodními partnery
- Pouze s obchodními partnery

13. Jaký je Váš názor na zabezpečení datové schránky?

Označte jen jednu elipsu.

- Nevyhovující, nedůvěřuji tomuto systému
- Průměrná, doufám v přiměřené zabezpečení
- Dobrá, nesetkal/a jsem se se žádným problémem
- Vyhovující, naprosto důvěřuji tomuto systému

14. Jste spokojeni se službami datové schránky?

Označte jen jednu elipsu.

- Ano
- Ne

15. Při jakých úkonech a jak často využíváte elektronický podpis?

*označte každý úkon od 0 do 5, kde 0=nevyužíváte vůbec a 5=využíváte nejčastěji

Označte jen jednu elipsu na každém řádku.

	0	1	2	3	4	5
Podepisování e-mailových zpráv	◯	◯	◯	◯	◯	◯
Zasílání elektronických faktur, dodacích listů a jiných účetních dokladů	◯	◯	◯	◯	◯	◯
Podávání daňového přiznání	◯	◯	◯	◯	◯	◯
Zasílání datových zpráv přes datové schránky	◯	◯	◯	◯	◯	◯
Archivace elektronických dokumentů	◯	◯	◯	◯	◯	◯
Přihlašování do systémů jako náhrada přihlašovacího jména a hesla	◯	◯	◯	◯	◯	◯

16. Využíváte elektronický podpis i při jiných příležitostech a pokud ano tak jakých?

_____

17. Využíváte-li elektronický podpis pro interní účely, o jaký typ se jedná?

Zaškrtněte všechny platné možnosti.

- ☐ Elektronický podpis
- ☐ Zaručený elektronický podpis založený na kvalifikovaném certifikátu
- ☐ Elektronická značka
- ☐ Elektronická značka založená na kvalifikovaném certifikátu
- ☐ Nevyužíváme

18. Zda využíváte při komunikaci s orgány státní správy elektronický podpis, tak s jakými?

Zaškrtněte všechny platné možnosti.

- ☐ Finanční úřad
- ☐ Obchodní rejstřík
- ☐ Katastrální úřad
- ☐ Celní správa
- ☐ OSSZ
- ☐ Jiné: _____

19. Jaký používáte prostředek při aplikaci elektronického podpisu?

Zaškrtněte všechny platné možnosti.

- [ ] USB token
- [ ] Čipová karta
- [ ] Jiné: _____

20. Jaká je dle Vašeho mínění největší výhoda elektronického podpisu?

Označte jen jednu elipsu.

- ◯ Úspora nákladů
- ◯ Jednoduchá a rychlá aplikace
- ◯ Zaručení zachování integrity dokumentu
- ◯ Zlepšení komunikace s orgány státní správy
- ◯ Jiné: _____

21. Jaká je dle Vašeho mínění největší nevýhoda elektronického podpisu?

Označte jen jednu elipsu.

- ◯ Komplikace při archivaci dokumentů
- ◯ Komplikace při konverzi dokumentů na listinou formu
- ◯ Náklady spojené s obnovou certifikátu
- ◯ Složitá obnova a používání certifikátu
- ◯ Nízká podpora
- ◯ Jiné: _____

22. Jak často využíváte elektronický podpis?

Označte jen jednu elipsu.

- ◯ Denně
- ◯ Alespoň jednou týdně
- ◯ Alespoň jednou měsíčně
- ◯ Jiné: _____

23. Co by se dle Vašeho názoru mělo na elektronickém podpisu změnit či vylepšit?

_____

24. Jaké jsou dle Vašeho názoru největší překážky pro širší využívání elektronického podpisu?

Označte jen jednu elipsu.

- ◯ Nedůvěřivost
- ◯ Nedostatek informací
- ◯ Vyšší pořizovací náklady v poměru k možnostem využití
- ◯ Složitý způsob pořízení certifikátu
- ◯ Nedostatečná podpora
- ◯ Jiné: _____