VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA
EKONOMICKÁ FAKULTA

KATEDRA PRÁVA

Aktuální problémy využití elektronického podpisu v praxi
Current Problems of Using Electronic Signatures in Practice

Student: Bc. Petra Šmídová
Vedoucí diplomové práce: Mgr. Bc. Adam Ptašnik, Ph.D.

Ostrava 2011

VŠB - Technická univerzita Ostrava
Ekonomická fakulta
Katedra práva

Zadání diplomové práce

Student: **Bc. Petra Šmídová**

Studijní program: N6208 Ekonomika a management

Studijní obor: 6208T011 Ekonomika a právo v podnikání

Téma: Aktuální problémy využití elektronického podpisu v praxi
Current Problems of Using Electronic Signature in Practice

Zásady pro vypracování:

1. Úvod
2. Teoretická východiska elektronického podpisu
3. Právní úprava elektronického podpisu
4. Elektronický podpis a jeho problémy v praxi
5. Závěr

Seznam použité literatury
Seznam zkratek
Prohlášení o využití výsledků diplomové práce
Seznam příloh
Přílohy

Seznam doporučené odborné literatury:

BOSÁKOVÁ, Dagmar et al. *Elektronický podpis: přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů.* 1. vyd. Olomouc: ANAG, 2002. 141 s. ISBN 80-7263-125-X.
BUDIŠ, Petr. *Elektronický podpis a jeho aplikace v praxi: certifikáty a certifikační autority, legislativní rámec elektronického podpisu, praktické aplikace.* 1. vyd. Olomouc: ANAG, 2008. 157 s. ISBN 978-80-7263-465-1.
MACKOVÁ, Alena a Bohumír ŠTĚDROŇ. *Zákon o elektronických úkonech a autorizované konverzi dokumentů s komentářem.* 1. vyd. Praha: Wolters Kluwer ČR, 2009. 528 s. ISBN 978-80-7357-472-7.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Mgr. Adam Ptašnik, Ph.D.**

Datum zadání: 25.11.2011
Datum odevzdání: 27.04.2012

JUDr. Bohuslav Halfar
vedoucí katedry

prof. Dr. Ing. Dana Dluhošová
děkanka fakulty

„Místopřísežně prohlašuji, že jsem celou diplomovou práci, včetně všech příloh, vypracovala samostatně“. Veškerou literaturu a další zdroje, z nichž jsem při zpracování čerpala, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Ostravě 27.4. 2012 Podpis…….

Děkuji Mgr. Bc. Adamu Ptašnikovi, Ph.D. za vedení a metodickou pomoc, kterou mi poskytl při zpracování diplomové práce.

Obsah

1. Úvod

Jako téma mé diplomové práce jsem si vybrala problematiku elektronického podpisu a s ním spojené výhody, nevýhody či nejrůznější problémy jeho praktického použití. Elektronický podpis je velmi diskutovaným tématem současné doby, ať již v bankovním prostředí, v souvislosti s ochranou dat dokumentů podepsaných tímto způsobem či věrohodností a uznáním listin využívajících elektronického podpisu.

Hlavním cílem diplomové práce je odhalení nedostatků elektronického podpisu jako takového, jakož i služeb souvisejících s elektronickým podpisem a rovněž problémů, které se týkají jeho zřízení a následného používání v praxi.

Diplomová práce zabývající aktuálními problémy využití elektronického podpisu v praxi je složena celkem z pěti samostatných kapitol. V části s názvem teoretická východiska elektronického podpisu budu podrobně analyzovat pojem elektronického podpisu a další skutečnosti, které se vztahují k této oblasti a jsou nezbytné k tomu, aby čtenáři pochopili, co elektronický podpis je a mohli se seznámit s jeho fungováním.

V další kapitole se zaměřím na právní legislativu elektronického podpisu v českém právním řádu. Stěžejním bodem bude především zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů. Dále se budu věnovat vyhláškám a to konkrétně vyhlášce 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. Poté zmíním vyhlášku č. 495/2004 Sb., kterou se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů. Další vyhláškou bude ta s č. 496/2004 Sb., k elektronickým podatelnám.

V neposlední řadě uvedu také Směrnici 1999/93/EC Evropského parlamentu a Rady, o zásadách společenství pro elektronické podpisy.

Čtvrtá kapitola bude zaměřena na velmi důležité praktické problémy elektronického podpisu, které zde budou podrobně popsány. V rámci této kapitoly bude provedena analýza praktických problémů elektronického podpisu prostřednictvím elektronického dotazníkového šetření u vybrané skupiny respondentů. Výsledky této analýzy budou přehledně popsány a také vyobrazeny na velmi srozumitelných grafech, které poskytnou jednoznačné odpovědi na dané otázky.

V závěru diplomové práce jsem logicky shrnula zjištění plynoucí z obsahu práce a nastínila možné návrhy a doporučení vedoucí ke zlepšení a zkvalitnění služeb elektronického podpisu v praxi.

2. Teoretická východiska elektronického podpisu

V této úvodní kapitole je nezbytné uvést základní pojmy, které se budou prolínat celou diplomovou prací týkající se problematiky elektronického podpisu v jeho související praxi. Samozřejmě stěžejní je objasnění skutečnosti samotného podpisu, elektronického podpisu a digitálního podpisu. V dalších podkapitolách se zaměřím především na typické vlastnosti elektronického podpisu, jeho druhy, certifikáty, které neodmyslitelně k elektronickému podpisu patří a v neposlední řadě také na certifikační autority, elektronické značky a časová razítka.

V současné moderní době se stále více distancujeme od užívání vlastnoručního podpisu v psané podobě. [3, str. 48-51] V souvislosti s pokrokovými trendy začíná převažovat u nejnovější dokumentace její elektronická podoba. Toto se netýká pouze nově vznikajících předpisů či nejrůznějších dokumentů, ale také ty stávající stále častěji mění svou podobu na tu elektronickou. Toho využívají nejen úřady při své komunikace s ostatními orgány, ale také občané či podnikatelé k usnadnění a především urychlení vzájemné, mnohdy zdlouhavé, komunikace.

2.1 Dokument v listinné a v elektronické podobě

V této podkapitole si přiblížíme základní rozdíly dokumentů v listinné a elektronické podobě a upřesníme, jaké skutečnosti jsou nepostradatelnou součástí oněch dokumentů.

Pro platnost určitého dokumentu v listinné podobě (písemnosti) je mnohdy vyžadován vlastnoruční podpis, v některých případech také ověřený vlastnoruční podpis, ať již notářsky, soudně či úředně.

Na rozdíl od dokumentů v listinné podobě existují také ty v podobě elektronické a k nim je ovšem nezbytný tzv. elektronický podpis. Každý z nás si dovede pod tímto pojmem představit téměř cokoliv, ale v podstatě není ničím jiným, než samotným řetězcem čísel. Není důvod k panice, jelikož s takovým řetězcem pracují v praxi pouze programy, které takovou podobu podpisu ověřují, a výsledek tohoto procesu je velmi uživatelsky přijatelný. Na následujícím obrázku je jasně viditelný výsledek programu Adobe Reader, který ověřil konkrétně vložený elektronický podpis. [7, str. 29]

V praktickém životě máme možnost se také setkat s jiným označením elektronického podpisu a tím je podpis digitální, který má rovněž povahu čísla a věcně by byl pro výklad

vhodnější[1]. V dikci zákonů a vyhlášek se tento pojem nepoužívá a z tohoto důvodu budu pro účely diplomové práce hovořit o podpisu elektronickém[2].

Pro účely zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů, se rozumí elektronickým podpisem údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě. [5, str. 282]

Definice elektronického podpisu vyplývající z výše zmíněného zákona má velmi obecný charakter a zahrnuje v sobě jak formy elektronického podpisu založené na asymetrické kryptografii, tak také jiné formy vyššího charakteru tohoto podpisu (zaručený elektronický podpis). [2, str. 112]

Je nutné poznamenat, a tak rozšířit definici pojmu elektronického podpisu, že tento druh podpisu je vždy připojen ke konkrétnímu elektronickému dokumentu a z tohoto tedy vyplývá, že je vyloučeno jej použít k podepsání jiných, byť zdánlivé shodných, písemností. Platí zde pravidlo, že ten, kdo zná soukromý klíč spojený s tímto podpisem je jediná osoba, kdo má elektronický podpis možnost vytvořit. Každá osoba bez výjimky se znalostí veřejného klíče podepisující osoby má schopnost si bezplatně a bez součinnosti třetí osoby (např. notáře) ověřit platnost konkrétního elektronického podpisu. [12, str. 150]

Elektronický podpis je ověřenou a bezpečnou metodou vzájemné komunikace, pomocí níž lze rozpoznat, zda probíhala manipulace se zprávou či s určitým datovým souborem. Tato výše popisovaná technika ve spojení s certifikátem jasně určuje seznámení podepisující osoby s obsahem dokumentu. [34]

[1] Přívlastek „digitální“ předurčuje zpracování něčeho v číselné, resp. číslicové podobě. Zatímco přívlastek „elektronický“ jasně svědčí o konkrétní prezentaci čísla, resp. číslice. Jako synonymum máme na mysli „optický“, „mechanický“ apod.

[2] V určitých případech se můžeme setkat s diametrálně odlišným výkladem pojmů. Za digitální podpis bývá označován takový podpis, u kterého je nezbytné založení na základě certifikátu a infrastruktuře veřejného klíče. Naopak elektronický podpis vnímáme v obecnějším duchu a certifikát k němu je potřebný jen za určitých okolností.

2.2 Podpis, elektronický podpis, digitální podpis

Jelikož je podpis jedinečným osobním údajem člověka a tedy se také týká každého z nás, je nezbytné věnovat se na počátku této diplomové práce co nejpřesněji jeho dostatečnému objasnění. Podpis jako takový je ve společnosti notoricky známá věc, ale jak je to s podpisem elektronickým? V této kapitole objasním, co se skrývá pod pojmem elektronický podpis, jaké známe jeho druhy, co považujeme za zaručený elektronický podpis a podpis uznávaný. V dalších podkapitolách dojdeme k výkladu bezpečnosti elektronické komunikace v praxi a základům kryptografie a neopomeneme ani problematiku certifikátů, certifikačních autorit, časového razítka či elektronické značky. [7, str. 28]

2.3 Druhy elektronických podpisů

V praktickém životě se setkáváme velmi často s problematikou důvěryhodnosti daného elektronického podpisu patřící k elektronickému dokumentu. Otázka spolehlivosti elektronického podpisu je diskutovaným tématem a to z důvodu velmi snadného vytvoření certifikátu k tomuto druhu podpisu každým z nás. Pomocí českého právního řádu definujeme nejrůznější druhy elektronických podpisů, a to vzestupně od nejméně důvěryhodného až po ten nejdůvěryhodnější:

- Elektronický podpis
- Zaručený elektronický podpis
- Zaručený elektronický podpis založený na certifikátu
- Zaručený elektronický podpis založený na kvalifikovaném certifikátu
- Zaručený elektronický podpis založený na kvalifikovaném certifikátu od akreditovaného poskytovatele certifikačních služeb (nejvhodnější pro styk s orgány veřejné správy)

V souvislosti s jednotlivými druhy elektronického podpisu máme možnost se dále setkat těmito důležitými pojmy, které je nutné zde uvést:

- Kvalifikovaný podpis – namísto kvalifikovaného podpisu je velmi často používán pojem zaručený elektronický podpis
- Vylepšený elektronický podpis – vylepšení spočívá ve skutečnosti využití jak základních funcích, které podpis nabízí, ale také navíc např. možnosti šifrování obsahu zprávy

- Kvalifikovaný podpis určený pro archivaci dat – jak vyplývá z názvu, funkcí je zejména dlouhodobé skladování určitých dat
- Hromadný podpis – principem tohoto druhu podpisu je podpisové schéma, které slouží k shlukování stávajících podpisů
- Kruhový podpis – pomocí kruhového podpisu je zjišťována příslušnost k dané skupině uživatelů. Příslušný dokument se zachováním anonymity podepisujícího člena je možné podepsat za celou příslušnou skupinu, ovšem s potencionálním nesouhlasem ostatních členů skupiny.
- Skupinový podpis – ve skupině oprávněných uživatelů slouží k „zamaskování" podepisující strany [28]

2.3.1 Zaručený a uznávaný elektronický podpis

Jako vyšší formu „klasického" elektronického podpisu označujeme zaručený elektronický podpis. Ta vychází z výše zákonem zmíněné formulace a říká, že je „zaručeným elektronickým podpisem elektronický podpis, který splňuje následující požadavky":

- Je jednoznačně spojen s podepisující osobou
- umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě
- Byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou
- Je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat,". [5, str. 528]

„Uznávaný elektronický podpis je zaručený elektronický podpis, založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb. Akreditovaným poskytovatelem certifikačních služeb je poskytovatel certifikačních služeb, jemuž byla udělena akreditace podle zákona." [34]

2.4 Elektronická komunikace v praxi

Elektronická komunikace a záležitosti s ní spojené jsou předmětem diskuse v posledních deseti letech. I přesto existuje v tomto krátkém období dělení na jisté etapy ve vývoji elektronické komunikace.

První etapou je praktické nahrazení klasické papírové korespondence základní elektronickou (především e-mailovou) komunikací. Dnes je tento druh komunikace běžný v obchodních kruzích i v klasickém dorozumívání mezi lidmi v občanském životě. Další

nespornou výhodou v prosazování elektronické komunikace je její bezpečnost, které dosahuje s využitím elektronického podpisu a dalších kryptografických metod. Stinnou stránkou je velké množství pošty, která pro nás nemá žádný praktický význam.

Druhou etapu reprezentují základní, jednoduché webové stránky poskytující konkrétní informace o dané společnosti prezentující se v internetovém prostředí. Pro mnoho firem je typické, že se nezabývali inovacemi svých webových stránek, ale setrvali v této druhé fázi a to například i několik let. Potenciální zákazníci nebo také obchodní partneři tak neměli možnost získat aktuální informace o jimi hledaném podniku.

Po prvních dvou fázích nastupuje poslední část vývoje zabývající se obchodním využíváním informací prezentujících se na síti a dostupných široké veřejnosti. Pro druhou etapu typické základní informace jsou postupně doplňovány o ty obchodní, údaje o daných produktech, jejich parametrech i cenách a dodací podmínky, které daná společnost využívá. Kvalitním zpracováním webových stránek může firma ušetřit spoustu nákladů a času. O tomto „prozření“ informují studie Českého statistického úřadu na téma Informační společnost v číslech za rok 2006 – 2008 (studie byly zpracovány v roce 2009). První tabulka se zabývá počtem podniku disponující vlastními webovými stránkami, přičemž jsou podniky rozděleny dle velikosti, dle ekonomické činnosti a dle místa registrace společnosti. Následný graf poukazuje na evropské státy a jejich podíl firem vlastnící webové stránky.

Přelomem při obchodování na internetu je samotný prodej určitého zboží či služeb, což klade samozřejmě obrovské nároky na technologii a také na bezpečnost této internetové služby. V raných fázích poskytování informací obchodník prostřednictvím internetu neznal svého zákazníka, nyní v rámci obchodování a placení za dodané zboží či služby je nutná identifikace zákazníka. S touto záležitostí souvisí dnes již běžné používání internetového bankovnictví a platby prostřednictvím něj. [2, str. 10-25] (Příloha 2, 3)

Elektronickou komunikaci lze rozdělit na:

- Aplikace B2B – obchodování prostřednictvím internetového rozhraní mezi obchodními partnery, firmami. Pro přenos velkého množství dat v relativně krátkém časovém období jsou využívány technologie založené na moderní kryptografii a certifikátech.
- Aplikace B2C – Business– to–Customers neboli e–shopy, internetové obchody apod. Aplikace B2C slouží k prodeji zboží či služeb koncovým zákazníkům. Je nezbytná integrace B2C s vnitřním informačním systémem obchodníka s cílem úspory nákladů.

- e – Government – elektronizace státní správy a samosprávy s výhodami v podobě rychlosti a kvality služeb občanům, uživatelské přívětivosti, úspoře nákladů i času. Do e – Government patří také problematika elektronických podatelen a datových schránek. Zákon o elektronickém podpisu v České republice definuje elektronickou podatelnu jako „pracoviště orgánu veřejné moci určené pro příjem a odesílání datových zpráv“, tedy jako prostředek komunikace mezi občanem a státní správou. Mimo ZoEP ČR zřízení elektronické podatelny upravuje také nařízení vlády ČR č. 495/2004 Sb.[3] Datové schránky lze chápat jako obdobu klasických poštovních schránek, přičemž komunikující osoby jsou ke schránkám připuštěny pouze dle autentizacích a autorizačních procedur (komerční certifikáty pro autentizaci přistupující osoby). Veškeré skutečnosti související s časem budou podloženy vytvořením kvalifikovaného časového razítka. Komunikující osoba má možnost využít zaručeného elektronického podpisu přenášených zpráv.
  [2, str. 21, 22.1.2012 – s. 12-25]

2.5 Bezpečná komunikace – základy kryptografie

Elektronická komunikace je již běžnou praxí, např. v oblasti veřejné správy, zdravotnictví, financí, obchodu či služeb. Takto přenášená data je ovšem nutné chránit, aby dosáhly shodné důvěryhodnosti jako na základě osobního styku. Jedná se zejména o ověření totožnosti, vlastnoručních podpisů nebo také skutečnosti týkající se uchovávání neboli archivace daných dokumentů. V souladu s mezinárodními normami se dbá především na důvěrnost informací, integritu (zabezpečení proti přepsání či úplnou změnu přenášených informací) a v neposlední řadě také nepopiratelnost (odpovědnost za autorství, vlastnictví, příprava odeslání zprávy a přijetí zprávy).

Ochranu informací lze chápat z pohledu ochrany dat u správce či uživatele, kdy jsou data pod výsadní kontrolou jediného uživatele (zabezpečení budov nebo ochrana daného počítače). Z jiného pohledu existuje ochrana logická, která využívá prvky kryptografie a s ní přidruženého šifrování. Přenos zašifrované zprávy je možné zhlédnout na následujícím obrázku. (Příloha 4)

[3] Nařízení stanovuje dle zvláštních právních předpisů zřídit elektronickou podatelnu takovým orgánům veřejné moci mající povinnost přijímat a odesílat datové zprávy se zaručenými elektronickými podpisy založenými na kvalifikovaných certifikátech, vydaných akreditovanými poskytovateli certifikačních služeb.

To, jakou kvalitu ochrany dosáhneme, závisí na výběru šifrovací metody s daným šifrovacím algoritmem, způsobem jeho aplikace a způsobem jeho využití za pomocí kryptografického protokolu. V praxi rozlišujeme symetrickou a asymetrickou kryptografii.

[2, str. 28]

2.5.1 Symetrická kryptografie

Symetrická kryptografie pracuje na základě jediného šifrovacího klíče, který je použit jak na straně odesílatele, tak na straně příjemce (k zašifrování i k dešifrování zprávy). Na počátku komunikace je nezbytné zaslat druhé straně šifrovací klíč zašifrovaný pomocí kryptografie s veřejným klíčem. V současném a v praktickém životě jsou využívány tzv. symetrické algoritmy a to v reálném čase. Opět si lze představit princip symetrické kryptografie pomocí následujícího obrázku. (Příloha 4)

Asymetrická kryptografie, kryptografie s veřejným klíčem

Rozdílem u této metody je použití dvojice klíčů neboli párových dat. Daný uživatel má možnost si tuto dvojici klíčů samostatně vygenerovat a to pomocí nejrůznějších softwarových produktů. Jestliže v praxi dojde ke zveřejnění klíče (veřejný klíč), aniž by došlo k odvození druhého klíče (soukromý klíč), je tato kryptografie označována jako kryptografie s veřejným klíčem, pro zjednodušení asymetrická kryptografie.

Princip této kryptografie spočívá v odhalení obsahu zprávy šifrované jedním z klíčů pouze se znalostí druhého z nich a naopak. Veřejný klíč je všeobecně známý, proto nemůžeme považovat šifrovanou zprávu soukromým klíčem za zcela chráněnou, jen za autorizovanou (nepopiratelnou). Tato metoda je také zákonitostí elektronického podpisu. Následující obrázek popisuje přenos neadresované, nezašifrované, ale autorizované zprávy. (Příloha 4)

K zajištění důvěrnosti zprávy se používá tzv. šifrování zprávy pomocí veřejného klíče adresáta. Obsah daného sdělení je tak chráněn a je přístupný pouze odesílateli a příjemci. Situace je znázorněna na následujícím obrázku. (Příloha 4)

A následně celý systém pro šifrování a podepisování zpráv pomocí asymetrické kryptografie čitelně ukazuje další vyobrazení. (Příloha 4)

2.6 Certifikáty

Certifikát veřejného klíče, zkráceně také certifikát, máme možnost z jistého úhlu pohledu chápat také jako analogii průkazu totožnosti, tedy nejčastěji občanského průkazu.

Certifikáty nejrůznějšího druhu, jak bude popsáno níže, se využívají zejména k řešení problému správy, distribuce a uchování klíčů.

Certifikáty vydané danou certifikační autoritou ve své nejzákladnější a také nejjednodušší podobě obsahují veřejný klíč, jméno a další osobní údajů, které zajišťují dostatečnou a jednoznačnou identifikaci subjektu vlastnící tento certifikát. V praxi běžně používané certifikáty nadále obsahují datum počátku své platnosti, datum jejího ukončení, jméno certifikační autority, která certifikát vydala, sériové číslo a v některých případech další upřesňující informace týkající se konkrétního certifikátu.

Nejčastějšími vydavateli certifikátů jsou specializovaní poskytovatelé certifikačních služeb (PCS), v praxi často známými pod názvem certifikační autorita (CA). Obecně však může být vydavatelem kdokoliv, kdo disponuje příslušnou specializovanou technologií, zpravidla ovšem upřednostňujeme výše zmíněné instituce.

V situaci certifikátů, u kterých existuje garance certifikační autority o jejich správnosti, je vyjmuta nutnost smluvní důvěryhodné výměny klíčů mezi dvěma subjekty. Vztah je založen pouze na dohodě o společně uznávané CA. [4]

Na straně klienta, při použití certifikační autority, jsou chráněná data redukována pouze na bezpečné uchovávání soukromého klíče. Ostatní skutečnosti jsou poté řešeny a střeženy pomocí certifikátů. Daný klient má možnost si ověřit certifikáty CA se znalostí veřejného klíče konkrétní CA. [2, str. 39]

2.6.1 Certifikáty CA

V úvodu této podkapitoly vztahující se k problematice certifikátů je důležité uvést a touto cestou si také ujasnit, že za vydání důvěryhodného certifikátu je zodpovědný její vydavatel, tedy certifikační autorita. Aby bylo možné spolehlivě ověřit, zda námi sledovaný certifikát vydala určitá CA, je nutné získat její certifikát. V tomto případě si musíme položit otázku, jak lze ověřit elektronický podpis na certifikátu CA a do jaké míry je certifikát CA důvěryhodný?

Z hlediska řetězce důvěry rozlišujeme dva druhy certifikátů CA. V prvním případě je nadřízenou institucí, jejíž důvěra je podložena zvláštním zákonem a není nutné ji prověřovat, prostřednictvím CA vydán certifikát s vyšší účinností. Instituce, která akreditované CA

[4] Bezpečná komunikace je umožněna i subjektům, u kterých postrádáme fyzické shledání či které nepodlehly vzájemné a složité důvěryhodné výměně svých klíčů.

certifikát vydala, ručí za jeho důvěryhodnost. „Certifikát CA je pak podřízeným certifikátem takové instituci.“

Ve druhém případě nastává situace shodného vlastníka a vystavitele certifikátu. Taková situace nastává ve skutečnosti, kdy si certifikát vydá CA sama. Jedná se o kořenové certifikáty (selfsigned – samopodepsaný certifikát), které samy o sobě nemohou zaručit pravost a důvěryhodnost certifikátu. Tu je zapotřebí získat odlišnou cestou. Prvním způsobem je předání certifikát vzájemně komunikujícím stranám a to důvěryhodným způsobem. Další možnou cestou je využití prostředníka a prostřednictvím něj tento certifikát zveřejnit.

Výše zmíněné řetězce důvěry jsou vyobrazeny na daném schématu. Tyto řetězce prezentují dvě základní cesty k získání certifikátu důvěryhodné CA. [2, str. 45-46] (Příloha 5)

2.6.2 Klientské certifikáty

Certifikační autority v mnoha případech vydávají nejrůznější druhy certifikátů dle přání a potřeb svých klientů. Pro bezpečnou komunikaci prostřednictvím internetového rozhranní máme na mysli nejrozšířenější typ certifikátu a to komerční certifikát.[5] Certifikátů tohoto typu je ročně certifikačními autoritami vydáváno desítky tisíc zejména z důvodů jejich velmi širokého uplatnění. Slouží především z technologického hlediska pro zajištění autentizace navzájem komunikujících stran prostřednictvím internetu či pro šifrování (zabezpečení důvěrnosti) daných zpráv, které se pomocí daného média přenášejí a pro účely diplomové práce zmíním nejdůležitější aspekt a tím je ochrana elektronického podpisu konkrétního klienta.

U komerčních certifikátů je nutné si uvědomit některé z velmi důležitých skutečností. Tento typ certifikátu není předmětem právní úpravy zákona prolínajícího se celou prací a z tohoto důvodu není jejich použití v praxi nikterak omezeno a účel jejich použití závisí pouze na komunikujících stranách a na vybrané technologii. U komerčních certifikátů je velice problematická důvěryhodnost a úroveň certifikačních autorit, která není nikým a ničím kontrolována a řízena. Velice běžné je použití certifikátů u elektronického bankovnictví nebo v oblasti komerčních aplikací.

Na opačném poli spektra rozeznáváme certifikáty vydávané v souladu se zákonem č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, které se nazývají certifikáty kvalifikované. Z české legislativy vycházející z evropských standardů je

[5] Tento typ certifikátu je takto označen z důvodu chybějící spojitosti se zákonem č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů

určeno jejich použití výhradně pro elektronický podpis. Velmi důležité je uvědomit si také nezbytnost kvalifikovaných certifikátů při elektronické komunikaci občanů se státní správou. Činnost certifikačních autorit vydávajících kvalifikované certifikáty je standardizována a kontrolována příslušnými výše postavenými úřady.

Do spektra kvalifikovaných certifikátů řadíme také kvalifikované systémové certifikáty, které splňují podmínky zákona o elektronickém podpisu, a jejich užití je spojeno s elektronickými podatelnami. Při použití kvalifikovaného systémového certifikátu máme na mysli elektronickou značku, nikoliv elektronický podpis.

Myšlení CA vedlo k vytvoření „balíčků“, které odstraňují nevýhody a naopak vyzdvihují výhody obou typů uvedených certifikátů. Je tak zajištěna legislativně kontrolována bezpečná elektronická komunikace a uživatelský komfort. [2, str. 52-62]

2.7 Certifikační autority

Certifikační autorita neboli poskytovatel certifikačních služeb je podle zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, vymezena jako fyzická osoba, právnická osoba nebo organizační složka státu, která vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy.

Certifikační autorita při vzájemné komunikaci dvou subjektů navzájem vystupuje jako třetí nezávislý a důvěryhodný „orgán“, svazující identifikaci subjektu (fyzickou identitu), pomocí jí vydaného certifikátu, s párem klíčů (elektronickou identitou), tedy následně s elektronickým podpisem. „Certifikační autorita garantuje jedinečnost subjektů podle užité identifikace subjektu v rámci vydávaných certifikátů. To je zajištěno legislativními a technickými pravidly provozu instituce CA.“ V případě splnění všech požadavků, certifikační autorita pomocí svého soukromého klíče stvrdí podpisem konkrétní dokument a vydá certifikát.[6] [2, str. 39]

Velice nezbytné je uvědomit si důležitou skutečnost ohledně odpovědnosti za poskytované služby. Certifikační autorita vydává nejrůznější typy certifikátů prostřednictvím daného subjekty či služby registračních autorit. I přesto, že vydávání certifikátů je zprostředkováno jinou institucí, certifikační autorita je naprosto vždy zodpovědná za jí poskytované služby třetím osobám, orgánům nebo podnikům. [1]

[6] Certifikát je podepsaným dokumentem a to jak z hlediska autorizace (CA je garantem pravosti jí vydaného certifikátu) a integrace dat (nelze zaměnit fyzickou osobu ani vlastníka certifikátu a jeho elektronickou identitu).

Další velmi důležitá skutečnost, kterou je nutné si uvědomit, souvisí s důvěryhodností certifikační autority. Důvěryhodnost certifikační autority je prvním krokem k bezpečné komunikaci prostřednictvím Internetu kdekoliv a s kýmkoliv. Pomocí služeb dané certifikační autority má uživatel jistotu, kdo se nachází „na druhé straně“, kdo je komunikačním protějškem. I přes přísná dodržení všech psaných i nepsaných pravidel dochází k problémům s identifikací komunikující osoby vlastnící a prokazující se certifikátem. V těchto případech je vhodné se s tímto požadavkem obrátit na certifikační autoritu disponující pojištěním pro tyto konkrétní záležitosti.

Na následujícím obrázku jsou zřetelně vyobrazeni akreditovaní poskytovatelé certifikačních služeb v České republice. Tento seznam zveřejňuje Ministerstvo vnitra ČR 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 koncepce a koordinace ICT ve veřejné správě, 26.8.2010

Obrázek 2.1: Poskytovatelé certifikačních služeb Zdroj: [32]

Česká republika udělila akreditaci Ministerstva vnitra třem kvalifikovaným certifikačním autoritám. Jak je patrné z vyobrazení, jsou jimi První certifikační autorita, a. s., Česká pošta, s. p. a eIdentity, a. s.

Česká pošta se na základě rozhodnutí Ministerstva informatiky České republiky stala akreditovaným poskytovatelem certifikačních služeb dne 3.8.2005. V současné době spadá problematika pod Ministerstvo vnitra, které kvalifikované certifikační autority spravuje. [22]

První certifikační autorita, a. s. (I. CA), která je v současnosti vlastněna několika významnými společnostmi[7], zahájila svou podnikatelskou činnost v roce 1996 pod záštitou portfolia produktů společnosti PVT, a. s. V rámci svého rozšíření byla v roce 2001 založena dceřiná společnost První certifikační autorita, a. s., která převzala veškeré činnosti a povinnosti týkající se poskytování certifikačních služeb od své mateřské společnosti. První certifikační autoritě, a. s. byla udělena akreditace pro výkon činnost akreditovaného poskytovatele certifikačních služeb ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů s účinností od 18.3.2002. Akreditaci udělil Úřad pro ochranu osobních údajů. [39]

Společnost identity, a. s. zahájila svou činnost počátkem roku 2004 s jasně definovanou vizí usnadnit a komplexně se orientovat na oblast správy elektronické identity. Od září roku 2005, kdy společnost získala akreditaci vystupovat jako akreditovaný poskytovatel certifikačních služeb, je velice nápomocná rozvoji bezpečné elektronické komunikace mezi nejrůznějšími subjekty. Jako příklad jmenujme zabezpečenou a věrohodnou komunikaci mezi jednotlivci, obchodními partnery či státní správou a samosprávou. [26]

2.7.1 Časové razítko

„Elektronické časové razítko (TS – Time Stamp) propojuje dokument, který je v elektronické podobě, s časovým okamžikem jeho vzniku.“ Zaručuje tedy, že konkrétně sledovaná data, která mají elektronickou podobu, v daný časový okamžik opravdu existovala. [24]

Časové razítko vydané poskytovatelem certifikačních služeb – časovou autoritou (TSA – Time Stamp Authority) je v praxi obdobou certifikátu a tedy elektronickým dokumentem. [2, str. 79]

Podle zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů je kvalifikovaným časovým razítkem datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem.

[7] Jsou jimi: Česká spořitelna, a. s., Československá obchodní banka, a. s., Telefónica Czech republic, a. s., Asseco Central Europe, a. s., Státní tiskárna cenin s. p.

2.7.2 Praktické fungování časového razítka

V případě, že člověk má zájem o zřízení časového razítka časovou certifikační autoritou, prvním krokem je zaslání této autoritě otisk dat (tzv. hash), pro něž jsou časová razítka vyhotovena. Jestliže je zaslaná žádost v naprostém pořádku, tedy obsahuje veškeré důležité náležitosti, je časovou autoritou vytvořena odpověď obsahující rovněž otisk dat doplněný o časový údaj, včetně dalších parametrů. Tato kompletní žádost je v tento okamžik poslána zpět žadateli. V praxi časové razítko zahrnuje přidělené sériové číslo, datum a čas a v neposlední řadě také identifikaci časové autority, v jejíž kompetenci bylo žádost posoudit a časové razítko vyhotovit a vydat. Výše uvedené údaje jsou poté připojeny k původním datům obsažených v žádosti, vše je stvrzeno elektronickým podpisem a zasláno žadateli zpět v podobě odpovědi na jeho prvotní požadavek. [24]

2.7.3 Použití časového razítka

Spojitost elektronického podpisu a časového razítka umožňuje vyjádřit velmi úzkou vazbu mezi daným člověkem a jím podepsaným dokumentem, ale také skutečnost přesného časového okamžiku, před nímž byla zaručeně prokázána existence daného dokumentu (časové razítko). Pro časovou autoritu je konkrétní dokument bezpředmětný, jelikož jej nemá k dispozici, disponuje pouze jeho otiskem, z něhož prakticky původní zprávu časová autorita nemá šanci získat a seznámit se s ní. Z tohoto důvodu nemusíme mít obavy z neoprávněného zásahu či přístupu cizí osoby k dokumentům opatřených razítkem této autority. [24]

2.8 Elektronická značka versus elektronický podpis

Elektronická značka je v související praxi obdobou samotného elektronického podpisu s rozdílem, že tato značka je podpisem vždy právnické osoby, na rozdíl od elektronického podpisu, kdy se v každém případě musí jednat o osobu fyzickou, která pouze zastupuje svou právnickou osobu. Elektronická značka je velmi často přirovnávána k firemnímu razítku dané PO. Typickým uživatelem jsou elektronické podatelny. [25]; [40]

Dle zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů se pod pojmem elektronická značka rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které splňují následující požadavky:

- Jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu

- Byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou
- Jsou k datové zprávě, ke které lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou

2.9 Výhody a nevýhody elektronického podpisu

S elektronickým podpisem a jeho praktickým zřízením a následným využíváním je spojena celá řada výhod, ale také jisté nevýhody, které budou součástí této podkapitoly týkající se teoretických podkladů tématu elektronického podpisu.

Mezi výhody elektronického podpisu patří:

- Nemožnost jeho zfalšování při správném a bezpečném použití oproti klasickému vlastnoručnímu podpisu
- Bezpečné stvrzení identity konkrétní podepisující osoby – příjemce je jasně srozuměn s osobou, která je autorem dané zprávy
- Prověření integrity zprávy (změna) – příjemce si je zcela jistý, že v průběhu transportu zprávy nedošlo k drobným či podstatným úpravám obsahu zprávy
- Nemožnost popření konkrétní zprávy – odesílateli je prakticky znemožněno popření tvrzení, že daná zpráva z jeho strany nebyla odeslána
- Nenapodobitelnost podpisu – podepisující osoba disponuje výsadní kontrolou svých potřeb nutných k podepisování dokumentů
- Efektivní, rychlá, snadná a pohodlná cesta komunikace s veřejnou zprávou
- V kombinaci s šifrováním zpráv nemožnost odhalení obsahu zprávy

Mezi nevýhody elektronického podpisu patří:

- Ochrana dokumentu – nutnost prevence zabezpečení dokumentu nejrůznějšími prostředky proti zkopírování dat v něm obsažených. Nezbytností je zálohování, ochrana a archivace listin
- Zabezpečení dokumentu – dokument je na své cestě od vystavitele k příjemci vystaven nepopiratelným rizikům. Kromě možného zneužití dat, můžeme jmenovat například pozměnění obsahu, změnu autora či časového údaje připojeného k dané písemnosti.
- Prokazatelnost důvěryhodnosti elektronického podpisu, elektronických značek, apod.

- Obcházení zabezpečení či kolize šifrovacích systémů
- Růst nákladů na zabezpečení elektronické komunikace
- Finanční náročnost zavedení – každá společnost má určitým způsobem svou elektronickou komunikaci vyřešenou a bez ní v konkurenčním prostředí prakticky nelze fungovat.
- Platby za prodlužování platnosti certifikátů
- Přístup k internetu
- Nedůvěra v elektronicky podepsanou písemnost
- Ztráta kontaktu tváří v tvář [30]; [29]

Již z výzkumu prováděného v roce 2006 bylo zjištěno, že popularita elektronického podpisu opravdu roste. „Ke konci letošního prvního čtvrtletí bylo v Česku přes sedmnáct tisíc aktivních elektronických podpisů s kvalifikovanými certifikáty“. [20]; [34]

2.10 Bezpečnost elektronického podpisu

Problematika bezpečnosti elektronického podpisu je nesmírně důležitá a často podceňována samotnými majiteli takto vytvořených podpisů. Na zabezpečení elektronického (zaručeného) podpisu má vliv zejména několik následujících parametrů. Prvním z nich zvolená ověřovací a podepisovací metoda (použitý algoritmus), bezpečnost naplnění námi vybraného algoritmu v konkrétním programu pracujícím s podpisy, jak dalece je důvěryhodná certifikační autorita (spolehlivost ověření vztahu mezi majitelem a veřejným klíčem) a v neposlední řadě způsob uchovávání soukromého klíče oprávněnou osobou. Spojitost zaručeného elektronického podpisu a dané fyzické osoby je z kontextu zcela zřejmá, každý z nás si z tohoto důvodu musí svůj soukromý klíč k elektronickému podpisu chránit a udržovat v bezpečnosti. V opačném případě čelí narušení soukromí a v závažnějších případech také zneužití svého podpisu. „Za hlavní rizika můžeme považovat:

- Odcizení privátního klíče (např. z počítače, je – li tam lehkomyslně uchován)
- Případ, kdy si vydavatel certifikátu neoprávněně zkopíruje data pro podepisování – soukromý klíč, případně je poskytne jiné osobě
- Padělání veřejného klíče odesílatele, resp. narušení jednoznačnosti vazby veřejného klíče na danou osobu, tj. za veřejný klíč dané osoby presentuje jiná osoba svůj podvržený veřejný klíč

Rozbití šifrovacího algoritmu (lze považovat pouze v krajních případech špatně provedeného vlastního algoritmu, u prověřených algoritmů používaných standardně pro digitální podepisování je to v reálném čase vyloučeno).“ [12, str. 151]; [31]

2.11 Využití elektronického podpisu v praxi

Elektronický podpis můžeme jako existující společnost či v občanském životě využít v mnoha oblastech. Jako příklad jmenujme bankovnictví a operace s ním spojené, komunikace mezi jednotlivými úřady či mezi úřadem a občanem, elektronické obchodování čili nakupování přes internet, apod. [4, str. 30-31]

Elektronický podpis a jeho služby využíváme v:

- Bankovnictví – v okamžiku zřízení internetového bankovnictví klientem dochází jak k úspoře nákladů klienta, ale také čau ze strany bankovního institutu, tak také k šetření času. Klient s touto službou nemá důvod navštěvovat banku a řídit se její otevírací dobou, ale má možnost všechny potřebné náležitosti vyřídit v pohodlí domova v kteroukoliv denní či noční hodinu. Úspora nákladů spočívá ve výrazně levnějších internetových službách než v prostředí banky či jiného institutu.
- Elektronické obchodování – díky elektronickému podpisu existuje při obchodování na internetu garance a jistota toho, že listiny či faktury nebyly cestou k příjemci (společnosti, od které výrobky nakupujeme) upraveny nebo zcela změněny. Zákazník, který využívá elektronického obchodování, šetří jak svůj čas, tak také své peníze. Má možnost si zboží prohlédnout v klidu, porovnat ceny obchodů a nakupovat v kteroukoliv dobu za jednoznačně výhodnější ceny než v kamenném obchodě.
- Státní správa a samospráva – opět se zde vyskytuje výhoda jmenovaná u dvou výše uvedených případů. Vnímáme úsporu nákladů jak úřadů při jejich komunikaci mezi sebou, tak také u občanů při dorozumívání s úřady nejrůznějšího typu. Zřízením elektronického podpisu odpadají náklady na tisk a šíření dokumentů a také je zde nesporně úspora času pracovníků úřadu, ale také občanů např. při podávání daňového přiznání nebo přihlášek či žádostí. [9]; [10, str. 7]

Z článku pana Zadražila periodické publikace Týden je zřejmé, v jakých případech máme možnost využít služby elektronického podpisu:

a) Přiznání k dani z příjmů, DPH, silniční dani a dani z nemovitostí
b) Komunikaci se zdravotními pojišťovnami

c) Komunikaci s OSSZ
d) Při podávání přihlášky k nemocenskému pojištění
e) Podání přehledu o příjmech a výdajích OSVČ
f) Podání evidenčního listu důchodového pojištění [11, s. 100-103]; [20]

3. Právní úprava elektronického podpisu

V třetí části diplomové práce se budu detailně zabývat právní úpravou elektronického podpisu. Jako stěžejní bude rozebrán zákon o elektronickém podpisu č. 227/2000 Sb., o elektronickém podpisu a o změně dalších zákonů. Následně bude zmíněna také nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu. Nemohu opomenout také vyhlášky o elektronických podatelnách a o postupech kvalifikovaných poskytovatelů certifikačních služeb. Na závěr této třetí kapitoly se budu věnovat směrnici 1999/93/EC Evropského parlamentu a Rady, o zásadách Společenství pro elektronické podpisy.

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

V zemích Evropské unie je klíčovým faktorem rozvoje certifikačních služeb jednotící prvek a tím je Směrnice 1999/93/EC. Jelikož se v rámci diplomové práce budu zabývat problematikou elektronického podpisu, významný pro mne bude zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů. Česká republika se ve spektru evropských zemí stala tou třetí, která zákon o užívání elektronického podpisu přijala a stalo se tak již v roce 2000. [2, str. 111]

Ministerstvo vnitra ČR je v současné době tím klíčovým kontrolním a bezpochyby také akreditačním orgánem, který má na starosti soulad v duchu se zákonem o elektronickém podpisu. Jeho kompetencemi je zejména dozor v oblasti řízení se zákonem o elektronickém podpisu, má také možnost udělit akreditaci poskytovatelům certifikačních služeb a vyhodnocuje shodnost nástrojů elektronického podpisu s požadavky udělenými výše zmíněným zákonem. [8] [2, str. 111]; [19]

Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) byl uveřejněn ve Sbírce zákonů 29.6.2000. Stěžejním smyslem zákona o elektronickém podpisu je především dát možnost užití digitálního podpisu v průběhu elektronické komunikace. Majitel tohoto druhu podpisu tak již nebude muset užívat

[8] Ministerstvo vnitra ČR upravuje postupy užívané poskytovateli certifikačních služeb 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).

podpisu vlastnoručního v rámci listinné formy dorozumívání. Hlavním podkladem pro vytvoření zákona o elektronickém podpisu byla již výše zmiňovaná směrnice Evropské unie 1999/93/EC ze dne 13.12.1999. [1, str. 122]

Mimo zákona o elektronickém podpisu existuje také novela zákona o elektronickém podpisu č. 440/2004 Sb., která nabyla účinnosti dne 26. července 2004. Novotou tohoto zákona je především pojem „kvalifikované časové razítko“, díky němuž máme možnost dokázat existenci konkrétního dokumentu v elektronické podobě a v čase a skutečnost použití „elektronické značky“. [9]

Novela zákona o elektronickém podpisu č. 101/2010 Sb. nabyla účinnosti dne 15. dubna 2010. V souvislosti s reakcí na rozhodnutí 2009/767/ES je udělena Ministerstvu vnitra ČR nová povinnost, která spočívá ve vedení a zveřejňování seznamu důvěryhodných certifikačních služeb. Zároveň s tímto novým závazkem, jsou kvalifikované certifikáty vydané v ostatních členských zemí EU, uznávány orgány veřejné moci v České republice. [37]

Účelem tohoto zákona je v souladu s právem Evropských společenství úprava používání elektronického podpisu, elektronické značky, poskytování certifikačních služeb a souvisejících služeb poskytovateli usazenými na území České republiky, kontrola povinností stanovených tímto zákonem a sankce za porušení povinnosti stanovených tímto zákonem. [5, str. 282 - 300]

Samotné použití elektronického podpisu v obecné rovině je upraveno také v zákoně č. 40/1946 Sb., občanského zákoníku a konkrétně v §40. V tomto paragrafu je uvedeno, že písemný právní předpis je platný v případě, že je podepsán jednající osobou. Z daného paragrafu plynu zrovnoprávnění dokumentů a také klasických podpisů i těch elektronických. Nutnost je dohoda smluvních stran na užití elektronického podpisu. [38]

3.1.1 Základní pojmy zákona o elektronickém podpisu

V této podkapitole se zaměřím na zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů a konkrétně na jednu z nejdůležitějších částí zákona a tím je vymezení pojmů. ZoEP – ČR definuje elektronický podpis jako „údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které slouží

[9] Pro elektronické značky stejně tak jako pro zaručený elektronický podpis se používá technologie digitálních podpisů. Přičemž elektronickou značkou může také PO a organizační složka státu označovat data.

jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě“. [2, str. 112]

Mezi další velmi důležité pojmy, které je nutné uvést k dosažení správného pochopení zákona, patří zejména datová zpráva, podepisující osoba, certifikát a poskytovatel certifikačních služeb.

Pod pojmem datové zprávy si představíme data v elektronické podobě, která lze také touto cestou přesunout či zaznamenat a uchovávat na záznamových médiích, které jsou využívány při zpracování a přenosu dat pomocí elektronické komunikace.

Podepisující osobou je fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby.

Certifikátem je datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu, nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její identitu.

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

Pozitivním přínosem technologie elektronických podpisů je zejména identifikace podepsané osoby a odhalení změny datové zprávy, tedy samotné porušení elektronického podpisu. [2, str. 116]

3.1.2 Povinnosti podepisující osoby a osoby spoléhající se na elektronický podpis

Zákon o elektronickém podpisu jasně a srozumitelně definuje povinnosti podepisující osoby, která je povinna:

- Zacházet s prostředky jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití
- Uvědomit neprodleně poskytovatele certifikačních služeb, který vydal kvalifikovaný certifikát, o tom, že hrozí nebezpečí zneužití jejich dat pro vytváření zaručeného elektronického podpisu.
- Bez zbytečného odkladu podávat přesné, pravdivé a úplné informace poskytovateli certifikačních služeb ve vztahu ke kvalifikovanému certifikátu.

Osoba spoléhající se na elektronický podpis není nikdo jiný než příjemce daného dokumentu opatřeného elektronickým podpisem. ZoEP – ČR nepřímo poukazuje na povinnost vykonání veškerých úkonů příjemcem zprávy pro ověření platnosti zaručeného elektronického podpisu a kvalifikované certifikátu. Úkony příjemce zprávy spočívají v ověření zaručeného elektronického podpisu a elektronické značky, v ověření platnosti certifikátu a ověření kvalifikovaného časového razítka. Veškeré tyto povinnosti jsou uvedeny v příloze vyhlášky č. 496/2004 Sb., o elektronických podatelnách. [2, str. 118-122]; [37]

3.1.3 Poskytovatelé certifikačních služeb

V této části diplomové práce se zaměřím na povinnosti poskytovatelů certifikačních služeb, které jsou pro ně závazné ze zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, konkrétně se tato úprava nachází v §6a.

Poskytovatel certifikačních služeb vydávající certifikáty je povinen:

- Zajistit, aby jím vydané certifikáty splňovaly veškeré podstatné náležitosti dle zákona
- Zajistit, aby údaje v certifikátech byly pravdivé a úplné
- Bezpečně ověřit totožnost osoby, která má daný certifikát získat
- Zjistit, zda osoba žádající o certifikát měla v době jeho vydání data pro vytváření elektronických podpisů
- Zajistit, aby měl každý možnost prověřit si identitu poskytovatele certifikačních služeb
- Zajistit veřejně přístupný seznam (i dálkový přístup) vydaných certifikátů, také těch zneplatněných, a aktualizovat jej
- Používat bezpečné systémy a zajistit postupy v souladu se zákonem a prováděcí vyhláškou
- Proti zneužití a padělání certifikátů přijmout opatření odpovídající vážnosti případu
- Vytvořit bezpečný systém uchovávání certifikátů v ověřitelné podobě

Podepisující osoba žádající o certifikát jej získá na základě písemné smlouvy, jiná forma smlouvy není přípustná, jinak je považována za neplatnou.

Poskytovatel certifikačních služeb nesmí dle zákona uchovávat ani kopírovat data, která mu byla podepisující osobou poskytnuta, pro vytvoření zaručeného elektronického podpisu. Dále je poskytovatel certifikačních služeb povinen oznámit veškerým subjektům, kterým poskytuje certifikační služby, o odnětí akreditace Ministerstvem vnitra ČR. Je nutné tuto informaci uvést také v seznamech. Poskytovatel musí na žádost podepisující osoby

ukončit platnost certifikátu a to z podnětu této osoby nebo v případě zjištění chybných či nepravdivých údajů.

Poskytovatel certifikačních služeb vede o každém svém úkonu provozní dokumentaci a zaměstnanci poskytovatele musí dle zákona zachovávat mlčenlivost o veškerých údajích, které se v rámci svého pracovně – právního vztahu dozvěděli. [40]

3.2 Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů

ZoEP – ČR je spjat s Nařízením vlády č. 495/2004 Sb. ze dne 25. srpna 2004, kterým se provádíí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů.

Vláda České republiky dne 25. srpna 2004 schválila nařízení k elektronickým podatelnám a tímto nařízením zavázala orgány veřejné moci ke zřízení e-podatelen. Tyto orgány mají povinnost, která vyplývá z nařízení vlády, vybavit své odborně proškolené zaměstnance zaručenými elektronickými podpisy a také zajistit bezpečný a pohodlný přechod informací „protékající“ těmito orgány.

Orgán veřejné moci v případě, že má zřízenou svou úřední desku, oznámí důležité a potřebné informace, které slouží k doručování datových zpráv tomuto orgánu. Příkladem těchto údajů mohou být kontaktní údaje, možnosti doručování datových zpráv, pravidla potvrzování doručení datových zpráv, technické parametry datových zpráv, apod.

[5, str. 301-303]; [33]

3.3 Vyhláška č. 496/2004 Sb. o elektronických podatelnách

Tato vyhláška ze dne 29. července 2004 určuje a dává orgánům veřejné moci za povinnost, jakým způsobem mají prostřednictvím elektronické podatelny přijímat a odesílat datové zprávy.

Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu je nadřízeným „orgánem“ vyhlášky č. 496/2004 Sb. o elektronických podatelnách. Toto nařízení, jak již bylo zmíněno výše, přikazuje zřídit elektronickou podatelnu a je návodem k naplnění podmínek dané nařízením. [5, str. 304-307]; [36]

3.4 Vyhláška č. 378/2006 Sb. o postupech kvalifikovaných poskytovatelů certifikačních služeb

Ve sbírce zákonů byla tato vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb zveřejněna dne 2. srpna 2006.

První část této vyhlášky určuje především postupy při vydávání kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek a slouží jako návod pro poskytovatele certifikačních služeb. Druhá část se zabývá ochranou soukromých klíčů a směřuje zejména k označujícím osobám, tedy orgánům veřejné moci.
[5, str. 308-327]; [35]

3.5 Směrnice 1999/93/EC Evropského parlamentu a Rady, o zásadách společenství pro elektronické podpisy

Tato část diplomové práce bude zaměřena na směrnici 1999/93/EC Evropského parlamentu a Rady. Bude uveden datum vzniku této směrnice a tedy i počátek závazku členských zemí k výstupnímu dokumentu, který je „jádrem“ této směrnice. V dalších částech této podkapitoly uvedu působnost směrnice, výklad určitých základních pojmů a také přínosy a využití této Směrnice v praktickém občanském i obchodním životě.

Elektronické podpisy již v dnešní praxi velmi úzce souvisí jak s elektronickou komunikací, tak také s elektronickým obchodem. Rozdíly v právní úpravě problematiky elektronického podpisu v členských zemích EU by mohly vytvořit vážnou překážku v používání elektronické komunikace a obchodování s pomocí těchto elektronických podpisů. Z těchto důvodů je nutné vytvořit jasný rámec Společenství, který bude jak v podnicích, tak v lidech podporovat a prohlubovat důvěru v elektronickou komunikaci, upraví podmínky vztahující se k elektronickým podpisům a vytvoří „pole“ důvěry v nové technologie a jejich obecné uznání ve společnosti.

„Tato směrnice neharmonizuje opatření týkající se služeb v oblasti důvěrných informací, které se řídí právními předpisy o veřejném pořádku nebo veřejné bezpečnosti jednotlivých členských států“. [1, str. 45] Naopak napomáhá k používání a k právnímu uznávání těchto podpisů skrz celé Společenství.

Cílem směrnice není harmonizace smluvních, ani záležitostí nesmluvní povahy, vztahů týkajících se elektronických podpisů. Tato směrnice je naopak zaměřena na co nejširší využití elektronických podpisů a jejich právní uznávání napříč celého spektra Společenství.

Hlavním zaměřením směrnice je správná funkce vnitřního trhu a to za pomoci stanovení právního rámce elektronických podpisů a vybraných certifikačních služeb. [1, str. 44-61]

Členské státy jsou dle této směrnice zavázány k umožnění volného oběhu produktů těchto podpisů a to na vnitřním trhu a mají za povinnost přijmout právní a správní předpisy s cílem souladu se směrnicí.

Dnem vyhlášení v Úředním věstníku Evropských společenství uvedená směrnice nabývá účinnosti, je určena členským státům a závazná pro členské státy je od 13. prosince 1999. [2, str. 102-110]; [1, str. 44-61]; [21]

4. Elektronický podpis a jeho problémy v praxi

Elektronický podpis v dnešní praxi již není zcela neznámým pojmem. Každý si pod ním dovede představit, co tento podpis znamená. První myšlenky mnohých z nás je, vlastnoruční podpis, ale v elektronické podobě. Problematika elektronického podpisu je ale složitější. Je pravdou, že užívání tohoto druhu podpisu se v poslední době stalo již velmi obvyklou a také v každodenním, jak soukromém, tak pracovním, životě jednoduchou záležitostí. Technologie elektronického podpisu v praxi přináší více výhod než nevýhod pouze v případě, že se uživatel je schopen bez problémů orientovat v základních pojmech, ve výběru aplikací, v procedurách souvisejících s certifikáty a jejich použitím a také v užívání párových dat. Nic na světě není dokonalé a proto i v záležitosti elektronického podpisu jako takové a jeho použití, uchovávání, uznatelnosti, apod., existuje řada problémů. Tyto problémy budou tématem praktické části diplomové práce. Tato tématika bude uchopena a vysvětlena co možná z nejvíce úhlů pohledu a tedy pro čtenáře srozumitelná a pochopitelná. Prvním problémem, který vyvstává, je trvalost elektronických dokumentů podepsaných právě zmiňovaným elektronickým podpisem.

4.1 Trvalost elektronických dokumentů

Z článku JUDr. Radima Polčáka, Ph.D. prezentovaného v právnickém tištěném periodiku Bulletin advokacie z měsíců července a srpna roku 2011 mne zaujala problematika trvalosti elektronických dokumentů.

Pan Polčák se ve svém článku zabývá použitelností elektronicky podepsaných písemností jako spolehlivých důkazních prostředků při nejrůznějších soudních líčeních, dále jsou zde velmi důkladně vysvětleny pojmy jako dokument, listina či nám pan Polčák objasňuje, jaké jsou např. základní funkce podpisu či jaké formy elektronického podpisu jsou uvedeny v zákoně č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu). Pro účely této diplomové práce, která se zabývá především analýzou problémů elektronického podpisu v praxi, mne bude velmi zajímat předposlední část tohoto článku a tou je trvalost elektronických dokumentů, jako jeden z nedostatků papírových písemností v elektronické podobě.

Virtualizace dokumentů nám kromě jiných skutečností přináší zejména přeměnu daných dokumentů co do jejich časové rovnováhy. Pro případy, kdy mají být určitým dokumentem dokazovány nejrůznější skutečnosti, je nutné disponovat takovými informacemi

jako v době pořízení tohoto dokumentu. V opačném případě nastává snížení jeho důkazní spolehlivosti a toto má za následek uplatnění námitky týkající se pravosti obsahu zmíněného dokumentu.

Ztráta informací zachycených na papírových dokumentech je věc samozřejmá. A to z důvodu žloutnutí papíru či blednutí inkoustu. Kvalita těchto listin tedy postupem čau ztrácí na ověřitelnosti jejich autenticity. Tento proces se ovšem nedá počítat na dny, týdny či měsíce, ale s určitou nadsázkou se jedná o stovky let.

Opačná situace nastává na straně elektronických dokumentů. Na tomto místě je nutné řešit problém datového nosiče a souborových formátů, které obsahuje inkriminované listiny. S technickým vývojem dochází k modernizaci obou těchto aspektů. V těchto případech se nejedná o neschopnost zpracování dříve běžně používaných datových formátů nebo datových nosičů (např. osmipalcová disketa), ale zpracování vyžaduje jak zvýšené úsilí pracovníků, tak také nemalé výdaje a v neposlední řadě také pravidelnou údržbu.

Mimo technických nedostatků spatřuje pan Polčák ve svém článku také problémy právního charakteru. Jako první uvádí „problém (trvalé) ověřitelnosti obsahu elektronických dokumentů včetně autentizací informace (podpisu nebo jeho náhražky)“. Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) zná úpravu zaručeného elektronického podpisu, ovšem se již nezabývá ověřováním a také uchováváním elektronicky podepsaných dokumentů. Shodným způsobem je precizně popsán postup podepisování listin, ovšem již bez typické zákonné úpravy ověřování pravosti takto podepsaných dokumentů. „Problém absence zákonné úpravy pro ověření pravosti zaručeného elektronického podpisu však spočívá v tom, že nelze v případě sporu postupovat na základě zákonných procedur a konstatovat pravost příslušného dokumentu a priori“.

Závažným problémem elektronických dokumentů v praxi je časová stabilita zaručeného elektronického podpisu jako takového. Pravost listin je možné ověřit pouze po dobu, kdy lze ověřit také pravost zaručeného elektronického podpisu. V průběhu několika desítek či stovek let může nastat problém, který spočívá v zániku historických systémových certifikátů nebo poskytovatele certifikačních služeb a to z důvodu ověření pravosti certifikátů na základě shodného systémového certifikátu, který byl již použit při ověřování původního podpisu. V krátkodobém horizontu je závažným nedostatkem změna systémových certifikátů, po dvanácti měsících od jejich vydání, a tedy touto skutečností dochází ke snížené ověřitelnosti zaručených elektronických podpisů již po jednom roce. Zaručený elektronický

podpis v praxi ztrácí na ověřitelnosti již např. v období mezi provedením elektronického podání a jeho zpracováním soudem nebo také mezi vydáním elektronického opisu soudního rozhodnutí a doručením tohoto opisu do datové schránky účastníka daného soudního řízení.

V těchto případech se nabízí možnost přepodepisování, ale zde je velký nedostatek v osobě, která musí podepsat jak původní, tak „nový“ dokument a také technickém zvládnutí celého procesu přepodepisování. Situaci neřeší ani tzv. časové razítko, jelikož to má za úkol pouze prokázat existenci dané listiny v čase, nikoli ověřovat pravost podpisů na ní. „ Jediné dlouhodobě perspektivní a ekonomicky reálné řešení průkazného zachování informační hodnoty elektronických dokumentů tak v současné době představují důvěryhodné systémy ukládání dat“. Máme na mysli takové technické standardy a takovou technologii, které mohou orgány veřejné moci v procesu aplikace práva považovat za spolehlivé, dostatečně zabezpečené a s vysokou mírou kontroly. Z výše zmíněného vyplývá, že elektronicky podepsané dokumenty jsou natolik kvalitní, nakolik je kvalitní technologie jejich uložení. Tyto systémy fungují takovým způsobem, že na počátku ověří, zda je dokument podepsán zaručeným elektronickým podpisem a pokud je shledána platnost tohoto podpisu, je listina uložena do systému na neomezeně dlouhou dobu. „Pravost dokumentu pak prokazujeme nikoli přímo, ale prostřednictvím toho, že dokument ležel v příslušném standardně zabezpečeném úložišti“. Na tomto principu pracuje také listinná spisová služba.

Je velmi nutné zmínit aktuální vládní návrh rekodifikace občanského zákoníku, který se v §510 odst. 2 zabývá právě spolehlivostí elektronicky podepsaných listin: „Má se za to, že záznamy údajů o právních jednáních v počítačovém systému jsou spolehlivé, provádějí – li se systematicky a posloupně a jsou – li chráněny proti změnám. Byl – li záznam pořízen při provozu závodu a dovolá – li se jej druhá strana k svému prospěchu, má se za to, že záznam je spolehlivý“.

Z článku pana Polčáka vyplývají následující závěry. Dodavatelé a uživatelé systémů, které se zabývají správou elektronických dokumentů, apelují na vznik a veřejné uznání technických standardů a základních institutů, které poté budou uznatelné orgány veřejné moci a také obecními soudy. S názory pana Polčáka jednoznačně souhlasím, jelikož problematiky služeb elektronického podpisu je rozebrána velice přehledně a návrhy řešení jsou logické a praktické pro ty, kteří se s elektronickým podpisem jako takovým setkávají denně. [8, str. 58-60]

4.2 Archivace dokumentů opatřených elektronickým podpisem

Archivace elektronicky zpracovávaných a předávaných dokumentů, které jsou opatřeny druhem podpisu, který je námětem celé diplomové práce, je jeden z nejzávažnějších a také prozatím neřešených problémů. Existuje samozřejmě archivace „klasická“, kterou se zabývá velké množství jak firem, tak také nejrůznějších úřadů. Jedná se o archivaci papírových dokumentů opatřených klasickým vlastnoručním podpisem určité osoby. Co se týče písemností, jejichž součástí je elektronický podpis, situace je mnohem složitější a odlišná.

Složitost archivace elektronických dokumentů spočívá zejména v množství požadavků, které jsou na ně kladeny. Těchto nároků je hned několik a je možné je rozdělit do samostatně prezentujících se částí. Mezi ty nejzásadnější patří dostupnost, čitelnost neboli prezentovatelnost a v neposlední řadě také jejich průkaznost.

Nejsnáze řešitelným problémem ze tří výše zmíněných je první z nich a to dostupnost elektronických dokumentů. V dnešní technicky vyspělé době již existují dokonale upravené aplikace, které usnadní uživateli či jakékoliv jiné instituci dostupnost dat a to jak strukturovaných, tak i nestrukturovaných dat. Tyto dostupné technologie se pyšní jak možností zálohování důležitých dokumentů podepsaných elektronicky, tak také jejich archivací, což je první problém týkající se problematiky elektronického podpisu jako takového a s ním souvisejících dokumentů.

Požadavky nejrůznějších obchodních a legislativních procesů se zaměřují na dostupnost elektronicky podepsaných dokumentů v řádkách desítek let, tedy po dobu minimálně 10 let. V případě papírových písemností je archivace v podstatě jednoduchou záležitostí. Samozřejmě i archivace těchto druhů dokumentů vyžaduje nemalé náklady, které mohou být zátěží nejrůznějších společností, úřadů, apod., dále se tato archivace neobejde bez předem stanoveného systému ukládání těchto dokumentů, vymezené prostorů pro jejich „skladování“ a také metodiku a realizování bezpečnostních požadavků, které jsou na společnosti a instituce kladeny. Jiná situace ale nastává u dokumentů pohybujících se v elektronickém světě. Deset let u papírových písemností se v technologicky vyspělé době nedá v žádném případě srovnat s deseti lety u elektronických písemností. Vyvíjení nových, překotných technologií, jak pro výměnu dat, tak také pro vývoj datových formátů, je velmi dynamickým odvětvím. Naposledy zmíněný vývoj a tím také změna a vylepšení datových

formátů zapříčiňuje nejrůznější problémy, konkrétně v zobrazitelnosti, čitelnosti či prezentovatelnosti dat, která jsou archivována již delší dobu.

Způsob archivace u papírových dokumentů jsou často v praxi velmi rozdílné oproti dokumentům opatřeným elektronickým podpisem, resp. elektronických dokumentů či písemností. V případě, že se společnosti či určité instituce chtějí, a mají takovou možnost, vyhnout problémům spojeným s archivací elektronických dokumentů, je vhodné používat osvědčené metody, formáty jednoduššího charakteru, které jsou všeobecně známy a také kvalitně popsány. Je nutné si také ověřit, zda formát používaný danou společností není úzce svázán s monopolním výrobcem či dokonce jedinou známou technologií. V neposlední řadě je vhodné si vybírat takové formáty pro archivaci, které jsou stále, tedy nepodléhají častým změnám. Vhodným textovým formátem pro společnosti vlastnící nejrůznější textové dokumenty, ale také např. pro úřady se jeví prostý textový formát (txt) či běžně používaný formát pdf. Oby tyto formáty byly schváleny jako standardy ISO (International Organization for Standardization).

Dále je nutné si pečlivě zvážit a uvědomit si při výběru výše zmíněného formátu dat nenáročnou aplikaci metod používaných především pro správnou a srozumitelnou prezentovatelnost dokumentů a to v delším časovém horizontu. Těmito metodami se budu zabývat v dalších částech diplomové práce. Jestliže je navíc požadováno, aby součástí daného elektronického dokumentu byl také (zaručený) elektronický podpis, musí vybraný formát podporovat konkrétní technologii. [2, str. 144-146]

4.2.1 Metody dlouhodobé archivace

Náplní této podkapitoly bude popis nejdůležitějších metod, které vedou ke snadné a dlouhodobé archivaci elektronických dokumentů. Metody se pokouší nalézt ideální řešení archivace, nýbrž každá z metod má své výhody a také nevýhody.

Metody dlouhodobé archivace lze dle určitého klíče a pro velmi snadné pochopení i pro laickou veřejnost rozčlenit do tří následujících kategorií. Jako první se v diplomové práci budu zabývat emulací. Emulaci v tomto kontextu chápeme jako emulaci funkcí starého systému systémem v novější verzi či podobě, přičemž je umožněno využití starších datových formátů, které by za jiných okolností v nových a aktualizovaných systémech nebylo možné v žádném případě použít a tak zobrazit dokumenty opatřené zmiňovaným elektronickým podpisem. Stejně tak jako ostatní metody, kterými se budu zabývat v dalších částech, i tato

metoda „naráží“ na technologický vývoj a jsou s ní spojeny především problémy technologického charakteru, čímž je omezena její funkce v praxi.

Další metodou, kterou je nutné zmínit, ale která bohužel není ideální z pohledu její využitelnosti v praktickém životě, je metoda založená na virtualizaci. Při tomto postupu je použit nízkoúrovňový jazyk, jehož vyjádření či prezentace je neměnná a to na počítačích, jež prošly již několika generacemi technického vývoje v oblasti IT.

Metoda migrace, která je poslední metodou, kterou v této podkapitole zmíním a která je na rozdíl od předcházejících metod považována za nejvýhodnější, co se týče jejího praktického použití. Princip metody migrace spočívá v přeměně dat staršího formátu do formátu nového, tedy v aktuální verzi. Při této metodě se postupuje obvykle danými kroky.

Prvním z nich je selekce vhodného typu datového formátu pro zobrazení elektronicky podepsaných dokumentů, ať již za soukromými nebo obchodními účely. Jestliže daný datový formát, který byl v předcházejícím kroku vybrán, není vhodný pro správnou a úplnou prezentovatelnost obsahu daného dokumentu, používá se v tomto případě výše zmíněná metoda migrace. Na základě existujících migračních schémat se písemnosti starého datového formátu migrují (transformují) do formátu nového a použitelného v současné praxi.

Tato poslední metoda se zdá být pro praktické použití ideální z pohledu její jednoduchosti, snadného použití a také prezentovatelnosti dat v novém formátu. Ale i tento postup má své nedokonalosti, které je nutné vyřešit. Jedním z těchto nejzásadnějších problémů je ztráta integrity[10] dat obsažených v daných dokumentech při procesu migrace. Ztráta celistvosti dokumentu je významný nedostatek, jelikož při ní dochází k narušení původního elektronického podpisu a v tomto případě také k narušení či úplné ztrátě bezpečnostních prvků, které jsou součástí elektronicky podepsaných písemností.

Určité řešení se nabízí ve vzniku zcela nové instituce, která by tuto migraci měla plně ve svých rukou. Při transformaci prováděnou touto institucí by samozřejmě docházelo k porušení původních bezpečnostních atributů souvisejících s elektronickým podpisem, ale touto migrací by byly vytvořeny nové, lepší a bezpečnější prvky chránící elektronicky podepsané dokumenty. Je ovšem nutné zajistit, aby tato instituce byla dostatečně důvěryhodná a aby nebylo možné pochybovat o průkaznosti a bezpečnosti migrovaných dokumentů.

[10] Dokumenty při procesu migrace ztrácejí svou integritu, tedy svou celistvost neboli neporušenost či nedotknutelnost.

Metoda migrace a tedy i teoreticky nově vzniklé instituce spočívají v ověření původních bezpečnostních prvků předložených listin a vydání potvrzení, které je následně přiloženo k transformovaným dokumentům. Výhodou tohoto postupu je, že původní písemnosti s bezpečnostními prvky se také archivují pro případné budoucí nahlédnutí.

Nejen dané dokumenty, ale také samotný elektronický podpis v průběhu času ztrácí svou důvěryhodnost z důvodu snížení bezpečnostních prvků kryptografických algoritmů. V tomto případě se nabízí řešení v podobě časových razítek a jejich opětovného použití u elektronických spisů.

S postupujícím technologickým vývojem neustále roste počet elektronických dokumentů nutných k archivaci. I přes pokroky v oblasti archivace elektronických písemností v okruhu standardizace (přijetí RFC – 4998 Evidence Record Syntax), „ideální“ řešení nebylo nalezeno. [2, str. 145-146]

4.3 Průkaznost provedené operace

Tato podkapitola diplomové práce se bude týkat průkaznosti provedených operací jak u papírových dokumentů, kde se jedná o mimořádně jednoduchou záležitost, tak také u elektronicky podepsaných písemností, kde je dokazování o něco složitější.

V případě papírových dokumentů je jak pro laickou, tak pro obchodní veřejnost velmi snadná průkaznost dané provedené operace. Jako příklad nám poslouží vklad určité sumy na účet klienta, kdy tento zákazník banky dostane od této operace doklad nebo každodenní situace nákupu zboží, kdy při této skutečnosti dostaneme v obchodním zařízení účtenku. Je tedy běžné, že jakmile obchodník, laická veřejnost či určitá instituce, provede závažné úkony, je možné, je, bez jakýkoliv problémů, doložit. Provedené operace jsou průkazné.

Jiná situace nastává v oblasti elektronických dokumentů opatřených elektronickými podpisy, kterými se zabývá celá diplomová práce. Jak již vyplynulo z předchozích odstavců této práce, zákon o elektronickém podpisu nám říká, že existuje spojitost mezi daným dokumentem a danou osobou, která má tuto písemnost k dispozici (elektronický podpis) a také, že tato listina je přístupná v určitém časovém okamžiku (časové razítko). Bohužel neexistuje prostředek, který by srozumitelně dokázal manipulaci s dokumentem a tím prokázal, že provedená operace je průkazná.

Samotný problém v oblasti průkaznosti provedené operace spočívá v dokazování odeslání, ale převážně v předání určitých dat. Nejhojněji využívaným prostředkem pro odesílání dat, je e-mail, jež není garantem toho, že tato zpráva byla předána. V některých případech není pomocí e-mailu možné zajištění doručení dat. V případech, kdy existuje potvrzení o přijetí odeslaných zpráv, kdy součástí je zaručený elektronický podpis, je průkaznost provedené operace doložena. Na tomto principu pracuje mnoho elektronických podatelen. [2, str. 146-147]

4.4 Mezinárodní uznatelnost elektronického podpisu

Mezinárodní uznatelnost elektronického podpisu je upravena ve Směrnici Evropského parlamentu a Rady 1999/93/ES o zásadách Společenství pro elektronické podpisy. Tato problematika je velmi závažná, jelikož zcela chybí obecně uznávaná a závazná pravidla, která by pohlížela shodně na požadavky na elektronický podpis v zemích EU.

Směrnice říká, že „členské státy mohou používání elektronických podpisů ve veřejném sektoru podmínit případnými doplňujícími požadavky“. Tato konkrétní věta obsažená ve Směrnici je vykládána v různých státech EU různě. Z toho vyplývá, že např. přiznání podané v jedné členské zemi a opatřené uznávaným elektronickým podpisem, nemusí být v jiném členském státě EU považováno za podepsané a důvěryhodné. A to ani přes další poznámku ve Směrnici, která říká, že „tyto požadavky musí být objektivní, průhledné, proporcionální a nediskriminační a musí se vztahovat pouze na zvláštní vlastnosti daného použití, nesmí vytvářet překážky při poskytování přeshraničních služeb občanům“.

Dalším problémem, který je spojen se Směrnicí Evropského parlamentu a Rady 1999/93/ES o zásadách Společenství pro elektronické podpisy je poskytování certifikačních služeb. Tento nedostatek existuje i přesto, že Směrnice říká, že „členské státy nesmí v oblastech, na které se vztahuje tato směrnice, omezovat poskytování ověřovacích služeb pocházejících z jiného členského státu“.

Závěrem této podkapitoly je nutné zmínit nesmírnou rozdílnost v posuzování elektronických podpisů v nejrůznějších státech EU a také nutnost zavedení sjednocovacích pravidel pro mezinárodní uznávání elektronických podpisů a to nejen v rámci zemí Evropské unie. [2, str. 147]

4.5 Analýza praktických problémů elektronického podpisu

V následující podkapitole se budu zabývat analýzou praktických problémů, které jsou spojeny s existencí elektronického podpisu a jeho používáním v praktickém životě. Pro tuto analýzu využiji marketingového výzkumu, který je považován za jeden ze základních informačních nástrojů. Podstatným prvkem tohoto marketingového výzkumu je poskytnout objektivní, kvalitní, pravdivé, relevantní a především aktuální informace o problémech elektronického podpisu v praxi. Marketingový výzkum je zpravidla členěn na dvě stěžejní fáze a to na fází přípravnou a realizační a je velmi podstatné, aby tyto fáze na sebe navazovaly, aby teda byla shledána jejich provázanost.

4.5.1 Přípravná etapa

Definování cíle a problému výzkumu

Marketingový výzkum v této diplomové práci se zabýval analýzou praktických problémů elektronického podpisu v praxi. Cílem mé diplomové práce bylo upozornit na aktuální problémy, které se vyskytují při zřízení a praktického používání elektronického podpisu. Cílem tedy bylo zjistit, jaké skutečné nedostatky v praxi existují, upozornit na ně a navrhnout řešení, jak by mohlo dojít k jejich odstranění a tím ke zjednodušení a zlepšení situace elektronicky podepsaných dokumentů. Samotné cíle byly vytvořeny v prvním týdnu marketingového výzkumu a to 3.2.2012.

Metoda marketingového výzkumu

Jako metodu uskutečněného marketingového výzkumu jsem si zvolila asi nejpoužívanější metodu elektronického dotazování. Elektronické dotazování bylo spuštěno 24.2.2012 a trvalo přesně dva týdny. Výhodou tohoto typu dotazování je především nízká finanční a časová náročnost pro tazatele. Na straně respondenta také existují určité výhody a to zejména důkladné promyšlení jednotlivých otázek a klidné prostředí na vyplňování. Existuje zde ovšem velká nevýhoda a tou je velmi nízká návratnost rozeslaných dotazníků.

V této diplomové práci se jedná o výzkum primární, jelikož jde o vlastní nalezení jednotlivých hodnot daných vlastností.

Technika výběru vzorku

Základním souborem byli všichni poskytovatelé právních služeb v Moravskoslezském kraji. Mezi tyto poskytovatele jsme zařadili advokáty, patentové kanceláře, exekutory a notáře. Jejich aktuální počet je, dle serveru Seznam.cz, 1468 ke dni 10.4.2012.

Výběrovým souborem bylo 250 respondentů z kategorií výše uvedených a nalezených pomocí internetových rejstříků firem poskytujících právní služby. Výchozí bylo použití webových stránek Seznam.cz a Google.cz. Vzhledem k opravdu nízké návratnosti jsem použila 100 zcela správně a úplně vyplněných dotazníků a to z důvodu specificky zaměřeného výzkumu analyzujícího praktické problémy elektronického podpisu. Jako techniku výběru vzorku jsem si zvolila techniku vhodné příležitosti, která usnadňuje tazateli výběr respondentů, kteří se shromažďují na velmi frekventovaných místech, např. u nákupních center, na nádražích či poskytují své údaje prostřednictvím webového rozhraní. [6, str. 158]

Nástroj sběru dat

Jako nástroj sběru dat pro tento konkrétní marketingový výzkum jsem použila mnou sestavený dotazník, který byl následně využit a odeslán na e-mailové adresy respondentů. Dotazník přeposílaný respondentům k vyplnění obsahoval úvodní odstavec, kterým jsem respondenty laskavě požádala o vyplnění následujících 15 otázek, ve kterých nechyběla na počátku otázka úvodní, dále jedna baterie, otázky filtrační, kontrolní a na konci otázky identifikační, které měly za úkol seznámit s osobou respondenta. Dotazník byl vytvořen ve druhém týdnu výzkumu a to 10.2.2012. (Příloha 1)

Předvýzkum

Předvýzkum neboli pilotáž je nedílnou součástí každého marketingového výzkumu, jelikož plní kontrolní funkci a má úkol odhalit špatné pořadí otázek, jejich nesprávnou formulaci či správný počet otázek. V tomto předvýzkumu jsem se rozhodla oslovit 10 podnikatelů Moravskoslezského kraje, jejichž e-mailové adresy jsem nalezla pomocí internetu a konkrétně webových stránek www.justice.cz a to dne 17.2.2012. Na základě této pilotáže byla k dotazníku připojena otázka dotazující se na znalost elektronického podpisu širokou veřejností a také doba použitelnosti elektronického podpisu související s obchodní činností.

Zpracování dat

Ke zpracování dat obsažených v řádně vyplněných dotaznících jsem použila programy Microsoft Word a Microsoft Excel.

Časový a věcný harmonogram

Aktivita	Týden								
	1	2	3	4	5	6	7	8	9
Sestavení cílů výzkumu									
Vytvoření dotazníku									
Pilotáž									
Sběr dat									
Zpracování, analýza dat									
Vyhodnocení údajů									
Návrhy řešení									

Obrázek 4.1: Časový a věcný harmonogram Zdroj: vlastní

4.5.2 Realizační etapa

Výzkum

V tomto marketingovém výzkumu zabývajícím se analýzou praktických problémů elektronického podpisu byl využit dotazník, jako nejčastější metoda sběru dat od respondentů.

Sběr dat obsažených ve výše zmíněném dotazníku probíhal ve čtvrtém a pátém týdnu výzkumu, konkrétně tedy od 24.2.2012 do 9.3.2012. Rozesláno bylo celkem 300 dotazníků na e-mailové adresy vybraných účastníků výzkumu, z nichž jsme zpracovali 100, řádně, zcela vyplněných dotazníků.

4.6 Vyhodnocení analýzy praktických problémů elektronického podpisu

Náplní této podkapitoly budou autorovy výsledky prováděného dvoutýdenního výzkumu a to jak v procentuálním vyjádření, tak také pomocí grafů a tabulek.

Zřízení elektronického podpisu

První otázkou v autorově dotazníku bylo zjišťováno, zda respondenti disponují a využívají služeb elektronického podpisu. Z výsledků dvoutýdenního výzkumu a z odpovědí na elektronické dotazování vyplynul jednoznačný závěr, a tedy, ve 100 % případů byla odpověď kladná. Respondenti, kteří elektronický podpis „nevlastnili“, odpověděli pouze na jim zaslaný e-mail a odmítli dotazník vyplňovat. Ze 100 oslovených respondentů odpovědělo 67 % mužů a tedy také logicky 33 % žen.

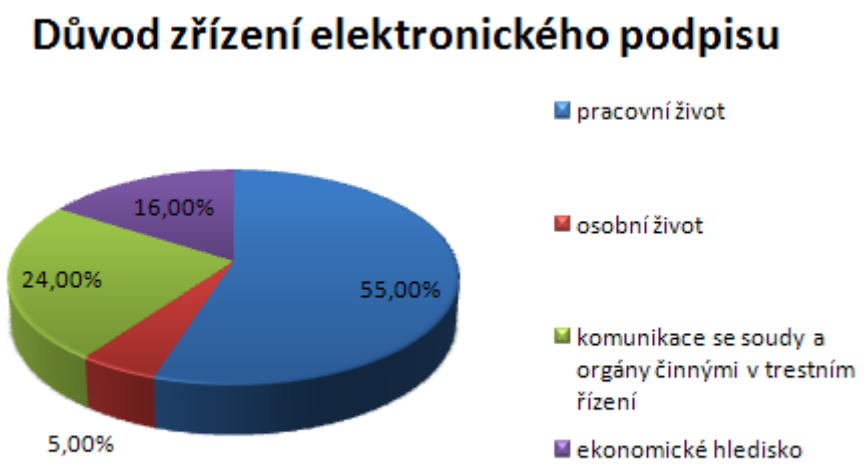
Důvod zřízení elektronického podpisu

Touto otázkou, ve které mohli respondenti označovat pouze jedinou vybranou odpověď, se autor snažil zjistit důvod pro zřízení elektronického podpisu a jeho následné používání v praxi u předem vybraného vzorku respondentů.

Nejfrekventovanějšími odpověďmi byla zmínka o prakticky každodenním využití služeb elektronického podpisu v pracovním prostředí, a to v 55 % případů. Vzhledem k vybranému vzorku oslovených respondentů, tedy advokátů a zaměstnanců advokátních kanceláří, dále exekutorů, patentových kanceláří a také samotných notářů a jejich zaměstnanců, bylo uvedení „pracovního použití“ elektronického podpisu pochopitelné. Velmi častým doplňkem k této zvolené možnosti bylo to, že se respondenti bez elektronického podpisu v pracovním životě vůbec neobejdou, je již neodmyslitelnou součástí jejich zaměstnání.

Osobní život, jako důvod pro založení a využívání elektronického podpisu, uvedlo pouhých 5 % respondentů. Respondenti osloveni k elektronickému dotazování jako druhý nejčastější důvod pro zřízení elektronického podpisu uváděli opět spojitost se svým zaměstnáním a to snadnější, rychlejší a zejména levnější komunikaci se soudy a s orgány činnými v trestním řízení. K této odpovědi respondenti zohledňovali zejména finanční hledisko a také nesporné ušetření času, které zřízením elektronického podpisu ušetřili.

Posledním nejfrekventovanějším důvodem pro to, aby si respondenti zřídili elektronický podpis, bylo ekonomické hledisko, u kterého se respondenti zmiňovali především o absenci úhrady poštovného při odesílání nejrůznějších dokumentů, ať již soudům či výše zmiňovaným orgánům činných v trestním řízení, se kterými jsou respondenti prakticky v každodenním „spojení“. Ekonomické hledisko jako důvod pro zřízení elektronického podpisu uvedlo 16 % respondentů.

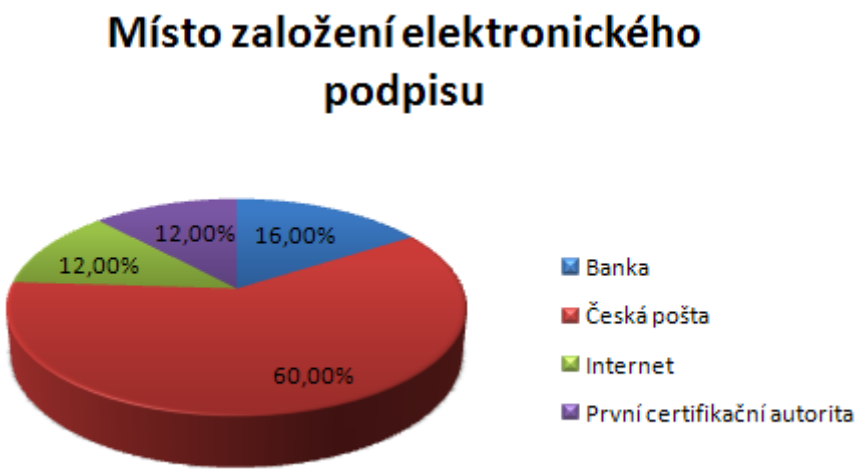


Graf 1: Důvod zřízení elektronického podpisu Zdroj: vlastní

Místo založení elektronického podpisu

Jako místo vhodné pro založení elektronického podpisu měli respondenti na výběr z 5, prakticky tedy 4 možností s jedinou možnou odpovědí a u poslední volby možnost rozepsání, kterou nevyužil žádný z respondentů. Odpověď, kterou respondenti nejčastěji volili, bylo výběr místa založení elektronického podpisu s využitím služeb České pošty, a to v absolutních hodnotách 60 ze 100 respondentů.

Na druhém místě se umístila Banka jako místo pro založení elektronického podpisu v procentuálním vyjádření s 16%. Shodně, a tedy po 12 % obdržela odpověď Internet a První certifikační autorita. Absolutní hodnoty jsou v případě tohoto výzkumu shodné s procentuálním vyjádření, jelikož autor zpracoval 100 řádně a zcela elektronicky vyplněných dotazníků. Elektronický podpis vydávají tzv. certifikační autority (Česká pošta s.p., První certifikační autorita. a.s. a eIdentity, a.s.) akreditovány Ministerstvem informatiky (nyní v kompetenci Ministerstva vnitra). Obrovský rozdíl mezi jednotlivými certifikačními autoritami je především v ceně jednotlivých poskytovaných certifikátů a také v pracnosti s jeho získáním a následným praktickým používáním.



Graf 2: Místo založení elektronického podpisu Zdroj: vlastní

Délka využití služeb elektronického podpisu

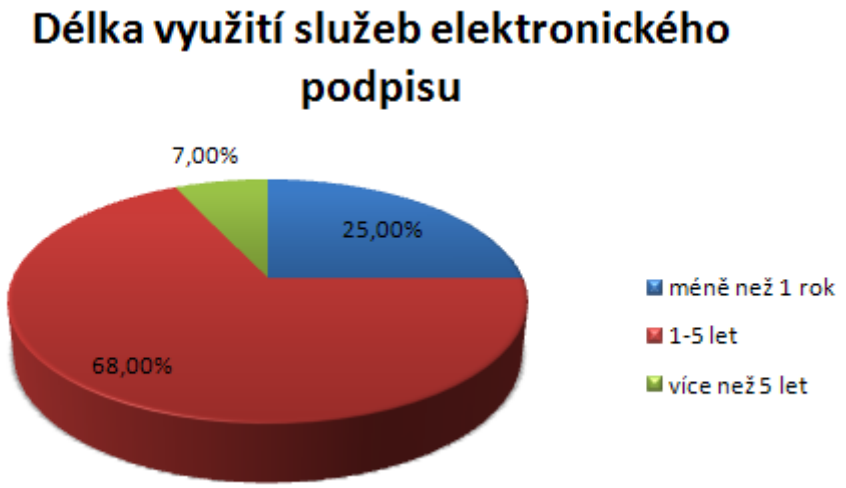
Další otázkou elektronicky publikovaného dotazníku určeného k vyplnění výběrovému souboru respondentů se autor snažil nalézt odpověď na to, jaká je délka využití služeb elektronického podpisu danými respondenty. Ti měli možnost zvolit si jednu z vybraných alternativ a to méně než 1 rok, 1 – 5 let a poslední možností bylo používání elektronického podpisu více než 5 let.

S 68 % hlasů se jako první umístila možnost délky využití elektronického podpisu s 1 – 5 lety. V absolutním vyjádření je tedy hodnota pochopitelně shodná s procenty uvedenými výše, tedy 68 respondentů označilo druhou možnost v této konkrétní otázce. Jako druhá skončila s 25 % možnost první a tedy, používání služeb elektronického podpisu respondenty méně než 1 rok. Délka využití služeb elektronického podpisu více než 5 let byla označena 7 % respondentů.

Problém u délky využití služeb elektronického podpisu tkví mimo jiné také v době jeho platnosti. Platnost jednotlivých certifikátů je 365 dní, tedy 1 rok, od jeho vydání a samozřejmě jsou zpoplatněny u každé z certifikačních autorit mnohdy až překvapivě odlišnou hodnotou. Platnost certifikátů se řídí Zákonem č. 137/2006 Sb., o veřejných zakázkách §140.

Velmi častým problémem, který respondenti uváděli v souvislosti s tímto výzkumem, byla nutnost prodloužení certifikátů vždy po uplynutí jednoho roku. Toto ovšem nemusí být tak namáhavou záležitostí, jelikož je možné celý proces provést elektronicky bez nutnosti osobní návštěvy jedné z certifikačních autorit. Uživatel v prvním kroku požádá certifikační autoritu o obnovení certifikátu, ta je poté vyzve k ověření emailových adres podobně, jak to

činila u prvotní registrace. Po těchto krocích již dochází k zaslání aktivačních údajů certifikační autoritou pomocí elektronické pošty (dané údaje jsou autoritou zaslány až po pečlivém ověření všech požadovaných údajů).



Graf 3: Délka využití služeb elektronického podpisu Zdroj: vlastní

Konkrétní problémy se zřízením elektronického podpisu

U tohoto konkrétního dotazu požadoval autor prostřednictvím dotazníku označení konkrétních problémů respondentů se zřízením elektronického podpisu. Respondenti měli možnost označit libovolný počet odpovědí dle vlastního uvážení a navíc také volbu „jiné“, která sloužila na podrobnější rozepsání problémů se zřízením elektronického podpisu, a to především v tom případě, kdy si respondent nevybral z předcházejících možností.

Složitost zřízení elektronického podpisu a jeho následné znovuobnovení byla nejčastěji zvolenou odpovědí na otázku, která zkoumala konkrétní problémy respondentů se zřízením elektronického podpisu. Tuto možnost, kromě dalších několika možných, zvolilo celých 34 % respondentů.

Nejzávažnější nedostatek, který respondenti spatřovali, byla nutnost obnovení kvalifikovaného certifikátu po 12 měsících jeho platnosti či zřízení zcela nového certifikátu u poskytovatele certifikačních služeb.

Z výsledků výzkumu vyplynul jasný závěr o akceptaci ceny při zřízení elektronického podpisu, jelikož cena jako jedna z možných odpovědí nevyhovovala pouze 1 % respondentů. Cena je odlišná u jednotlivých certifikačních autorit, tedy u služeb České pošty s.p., u První certifikační autority, a.s. a u eIdentity, a.s.

U České pošty se cena za jednotlivé druhy certifikátů pohybuje od 348 Kč za komerční osobní certifikát, až po kvalifikovaný systémový certifikát (elektronická značka) s cenou 1 788 Kč, veškeré s platností 365 dní.

V ceníku První certifikační autority nalezneme hodnoty od 395 Kč za komerční certifikát až po částku 780 Kč za kvalifikovaný systémový certifikát. Z tohoto je jasně patrné, že např. u kvalifikovaného systémového certifikátu je cena odlišná o více než 1 000 Kč. U komerčních certifikátů je rozdíl zanedbatelný.

Nejmarkantnější rozdíly v ceně kvalifikovaného systémové certifikátu lze spatřit u třetí certifikační autority, tedy eIdentity, a.s., kdy částka tohoto certifikátu šplhá na neuvěřitelnou výši 3 480 Kč. Vzhledem k předchozím dvěma autoritám je rozdíl v ceně značný. Komerční certifikát u eIdentity, a.s. má hodnotu 354 Kč.

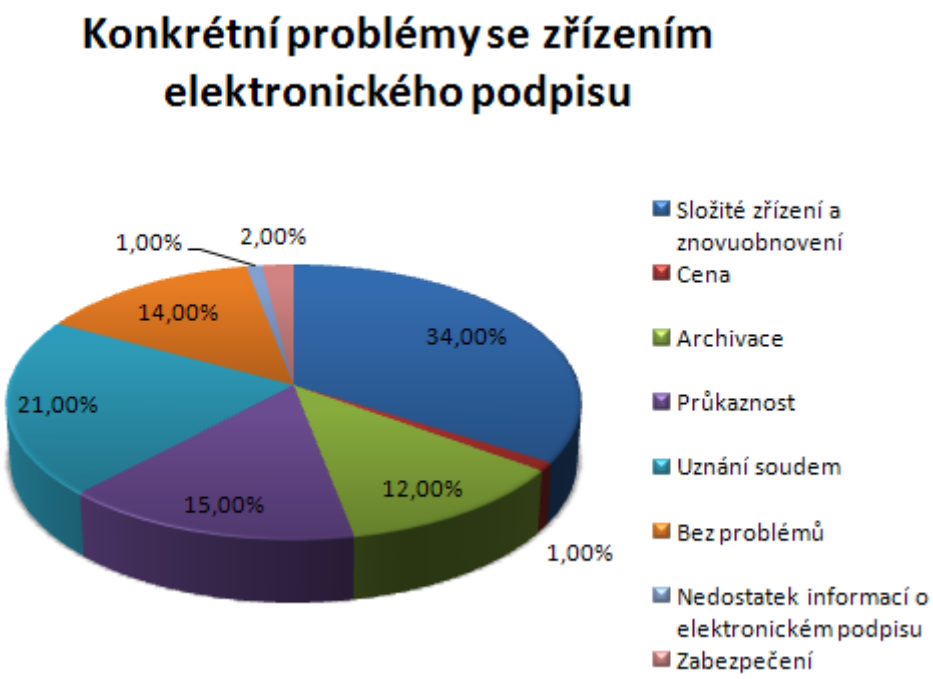
Archivaci je zejména velmi úzce spjata s neustálým zájmem o vývoj v oblasti IT, jelikož ten má zásadní vliv na metody archivace elektronicky podepsaných dokumentů. Problém s archivováním elektronických dokumentů má 12 % respondentů.

Průkaznost se stala dalším závažným problémem, který respondenti spatřovali u služeb elektronického podpisu. Tuto možnost odpovědi zvolilo 15 % dotázaných. Průkaznost elektronicky podepsaných dokumentů a závažné problémy s ní, jak již bylo uvedeno v předchozích částech diplomové práce, tkví v nemožnosti doložitelnosti manipulace s daným elektronickým dokumentem.

Praktický nedostatek, který se velmi často objevuje, spočívá v neuznání elektronicky podepsaných dokumentů soudem a to ve 21 % tohoto výzkumu. Tato skutečnost může mít za následek například neuznání elektronicky podepsaných písemností soudem jako důkaz v líčení a následně prohraný soudní spor.

Respondenti oslovení v rámci tohoto výzkumu ve 14 % případů neshledali žádný konkrétní problém se zřízením elektronického podpisu.

Zabezpečení jako problém spatřovaly 2 % respondentů a po 1 % získal problém, kdy dotázaní uváděli, že nemají či neměli dostatečné množství informací o elektronickém podpisu, tudíž pro ně zřízení této služby bylo náročné.



Graf 4: Konkrétní problémy se zřízením elektronického podpisu Zdroj: vlastní

Konkrétní problémy s používáním elektronického podpisu

Cílem šesté otázky tohoto elektronického dotazování bylo zjistit konkrétní problémy, které respondenti zaznamenali při používání služeb elektronického podpisu.

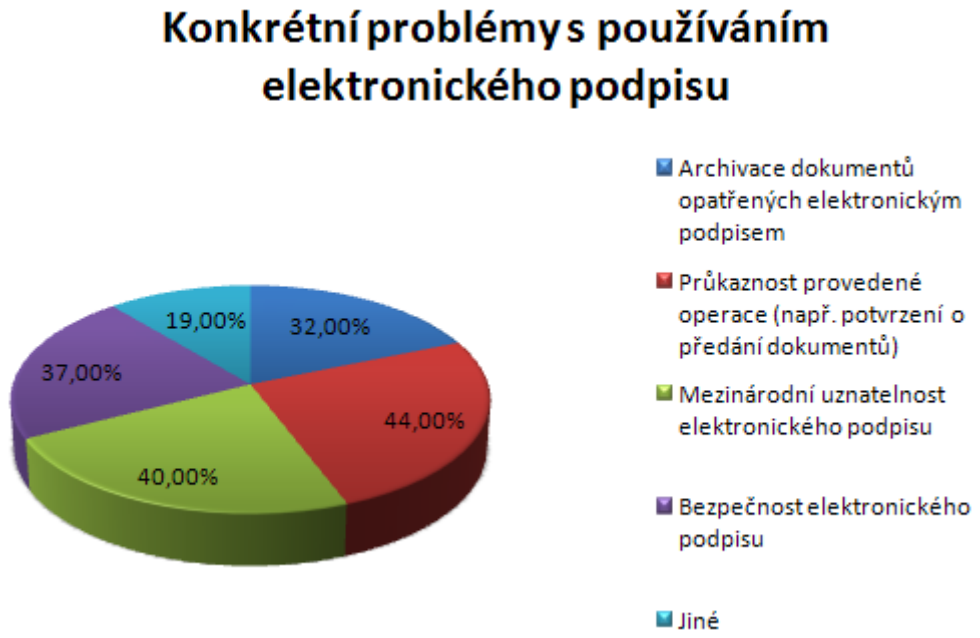
Nejzávažnějším nedostatkem, který dotazovaní označili, byla průkaznost provedené operace. Tedy, jak již bylo uvedeno v předchozí otázce a také v podkapitole zabývající se problémy elektronického podpisu v praxi, dokázání skutečnosti manipulace s daným dokumentem opatřeným elektronickým podpisem. Tuto možnost zvolilo 44 % respondentů.

Druhou volbou, kterou respondenti označili ve 40 % případů, se týkala mezinárodní uznatelnosti elektronického podpisu. Tato situace spočívá především v odlišné legislativě České republiky a ostatních zemí, kde si respondenti přejí využívat dokumenty opatřenými elektronickými podpisy (certifikáty zakoupeny u jedné ze tří certifikačních autorit v ČR). Je patrné, že chybějící legislativa, která by shodně pohlížela na elektronický podpis, je závažným nedostatkem.

Zabezpečovací mechanismy, které mají za úkol chránit před zneužitím elektronického podpisu, jsou problémem při používání tohoto druhu podpisu v 37 %. Ti respondenti, kteří si vybrali tuto možnost v jedné z následujících otázek také uvedli, že se domnívají, že elektronický podpis a veškeré služby, které s ním souvisí, nejsou bezpečné. Obávají se o zneužití svého podpisu neoprávněnými osobami.

Archivace dokumentů opatřených elektronickým podpisem bývá považována za největší problém, který souvisí s používáním tohoto podpisu. V tomto výzkumu, jej označilo 32 % respondentů.

Možnost volby „Jiné“ zvolilo 19 % respondentů. Přesto, že se u této odpovědi mohli rozepsat, neučinili tak.

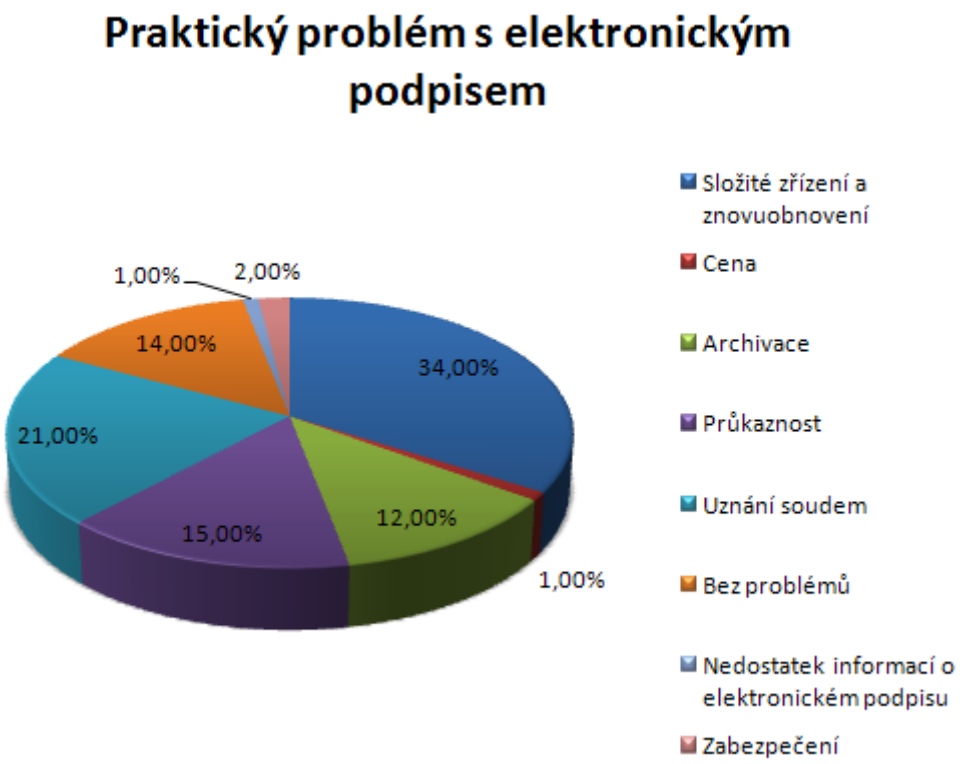


Graf 5: Konkrétní problémy s používáním elektronického podpisu Zdroj: vlastní

Praktický problém s elektronickým podpisem

Cílem další otázky v elektronickém dotazníku bylo zjištění dalších praktických problémů, se kterými se oslovení respondenti setkali a které doposud nebyly uvedeny v předchozích odpovědích na otázky číslo 5 a 6.

Z výsledků je patrné, že koláčový graf je shodný s grafem otázky číslo 5, jak procentuálním vyjádření, tak také absolutním. Je tedy bezpředmětné opakovat již to, co bylo uvedeno výše. Respondenti nezaznamenali žádné další problémy jiné než ty uvedené ve výčtu možností otázce 5 a 6.



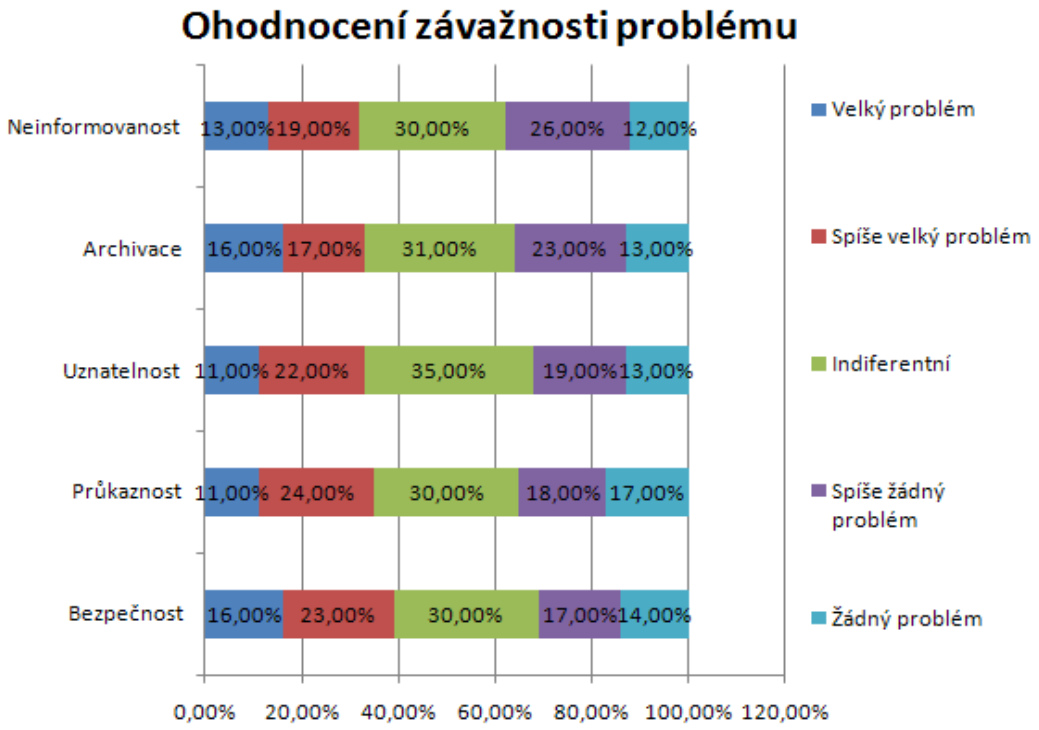
Graf 6: Praktický problém s elektronickým podpisem Zdroj: vlastní

Ohodnocení závažnosti problému

Ohodnocení závažnosti problému týkajícího se elektronického podpisu a jím podepsaných dokumentů bylo náplní další otázky v elektronicky rozesílaném dotazníku. Respondenti měli za úkol označit závažnost problémů známkami od 1 do 5, stejně tak jak je to notoricky známé ze školního prostředí. Pod známkou 1 se skrýval velký problém vnímaný respondenty a pod známkou 5 naopak žádný problém. Jak je patrné z následujícího grafu, respondenti používali nejčastěji známku 3, která měla upozornit na to, že dotázaní v dané oblasti nevidí obzvlášť závažný problém, ale rozhodně nejsou k dané problematice lhostejní.

Bezpečnost elektronického podpisu získala průměrnou známku 2,9 s procentuálním ohodnocením ve výši 16 %. Dalším kritériem byla průkaznost, jejíž známka činila 3,06 a 11 %. Třetím činitelem se stala uznatelnost, která u respondentů získala v průměru známku 3,01 v procentuálním hodnocení opět 11 % jako u předchozí možnosti. Předposledním možností, kterou měli respondenti ohodnotit, se stala archivace, která skončila s průměrným hodnocením přesně 3 a 16 %, stejně tak jako otázka bezpečnosti. Neinformovanost, tedy nedostatek podstatných informací o celé problematice elektronického podpisu vidí 13 % respondentů jako závažný nedostatek, průměrná známka tedy činila 3,05.

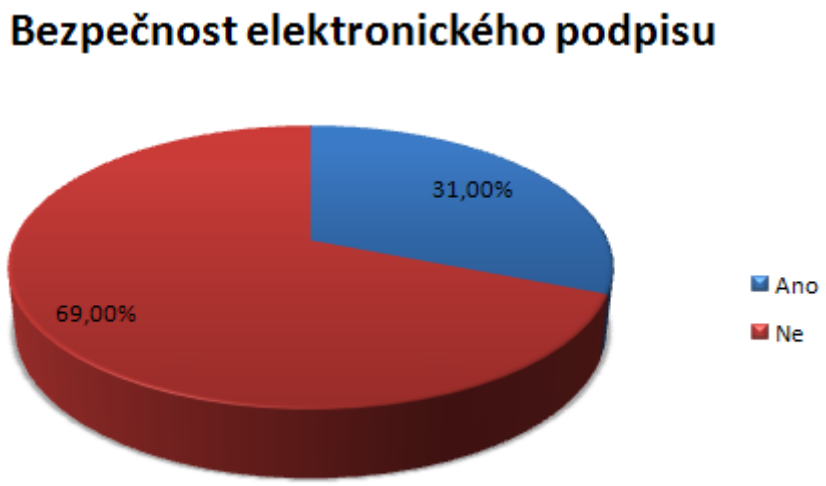
Velká řádka respondentů ovšem u této otázky zvolila tzv. „zlatou střední cestu“. Jejich hodnocení se pohybovalo od 30 % u možností týkající se otázky bezpečnosti, průkaznosti a neinformovanosti, až po 31 % za volbu archivace a 35 % u závažnosti uznatelnosti elektronicky podepsaných písemností.



Graf 7: Ohodnocení závažnosti problému Zdroj: vlastní

Bezpečnost elektronického podpisu

Otázka bezpečnosti elektronických dokumentů a tedy samozřejmě i elektronického podpisu byla řešena v několika předchozích otázkách. Tato konkrétní otázka jen shrnuje to, co již bylo řečeno v předcházejících odstavcích. Respondenti, přesně 69 % z nich, se domnívají, že elektronický podpis jako takový není zcela bezpečnou záležitostí. Tito respondenti mají oprávněné obavy, že jejich podpis bude zneužit či s ním bude neoprávněně nakládáno. Naopak 31 % dotázaných elektronickému podpisu věří a bez obav jej používají ve svém každodenním pracovním životě.



Graf 8: Bezpečnost elektronického podpisu Zdroj: vlastní

Povědomí elektronického podpisu u veřejnosti

Otázka elektronického dotazníku, která se zabývala povědomím problematiky elektronického podpisu u veřejnosti a znalost jeho funkcí, dopadla jednoznačně. Výsledku 30 % dostála odpověď ano, tedy toto množství respondentů si myslí, že elektronický podpis je u veřejnosti velmi známý a také, že veřejnost zná např., k jakému účelu v podstatě elektronický podpis v praktickém životě slouží.

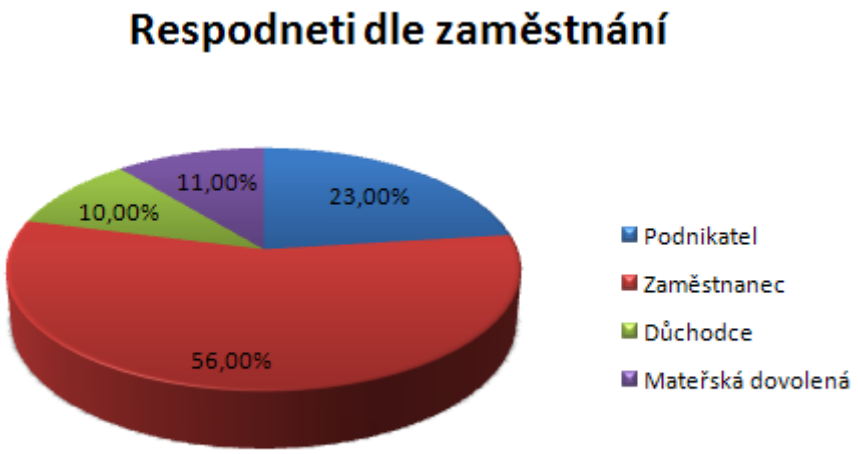
Naopak velké množství dotázaných je přesvědčeno o absolutní neznalosti elektronického podpisu a jeho funkcí veřejností. Respondenti se domnívají, že tzv. laická veřejnost netuší, jakým způsobem a na jakých místech si elektronický podpis zřídit, jaká je jeho platnost, typy podpisů, které jsou nám k dispozici a také především, jaké je jeho spektrum použití a jak usnadní pracovní život např. OSVČ nebo právnickým osobám.

Respondenti dle zaměstnání

Otázka číslo 11 se snažila zjistit, jaké skupiny obyvatel se do elektronického dotazování zapojily. Nejpočetnější skupinou se stali zaměstnanci jak advokátních kanceláří, tak také ti, kteří jsou zaměstnáni v kancelářích notářů, exekutorů či patentových kancelářích. Zaměstnanců se tedy zúčastnilo celých 56 %.

Druhou důležitou skupinou se stali podnikatelé s 23 %.

Za nimi se umístily ženy, případně muži, na mateřské dovolené s 11 %, kteří tedy před odchodem na mateřskou dovolenou byli podnikateli či zaměstnanci oborů uvedených v další otázce dotazníku. Poslední skupinu tvoří důchodci s 10 %, kteří spadají, respektive spadali, do jednoho z oboru činností uvedených níže.



Graf 9: Respondenti dle zaměstnání Zdroj: vlastní

Respondenti dle oboru činnosti

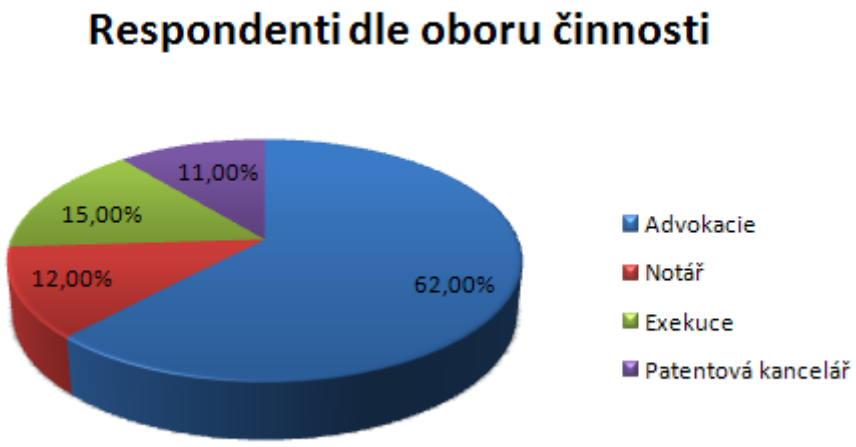
Další v pořadí 12 otázka výzkumu, který se zabýval analýzou problémů elektronického podpisu, byla tzv. otevřená otázka, při které měli respondenti možnost se rozepsat v jimi uváženém rozsahu. Otázka zněla takto: „Kde konkrétně pracujete? (rozepište, např. název společnosti a obor)“

Výsledky této konkrétní otázky dopadly jednoznačně ve prospěch oboru advokátů, jelikož tato skupina respondentů řádně a zcela vyplnila elektronický dotazník a to v 62 % případů. Jelikož respondenti byli vybíráni pomocí webového serveru Seznam.cz a jeho aplikací s názvem „Firmy“, jsou výsledky pochopitelné. V Moravskoslezském kraji je na www.seznam.cz v sekci Firmy a podsekci právní služby registrováno 1 356 advokátů.

Druhou početnou skupinu tvořili respondenti působící v oblasti exekuce, kteří byli vybráni shodně jako skupina advokátů pomocí, v České republice velmi známého a také jednoho z nejpoužívanějších vyhledávačů, Seznam.cz. Exekutoři v rámci tohoto dotazování byli zastoupeni 15 %.

Třetí velmi početnou skupinu tvořila skupina notářů, kterých bylo v den dokončení elektronického dotazování na webovém vyhledávači Seznam.cz v rámci Moravskoslezského kraje celkový počet 76. Všem těmto respondentům byl odeslán elektronickým způsobem dotazník určený k vyplnění. Řádně vyplněný dotazník odeslalo nazpět 12 notářů z našeho kraje. V procentuálním vyjádření samozřejmě 12 %, stejně tak jako vyjádření absolutní.

Poslední početnou skupinu tvořily patentové kanceláře, které až na jednu z nich zcela vyplnily jim poslaný dotazník a to v 11 % případů.



Graf 10: Respondenti dle oboru činnosti Zdroj: vlastní

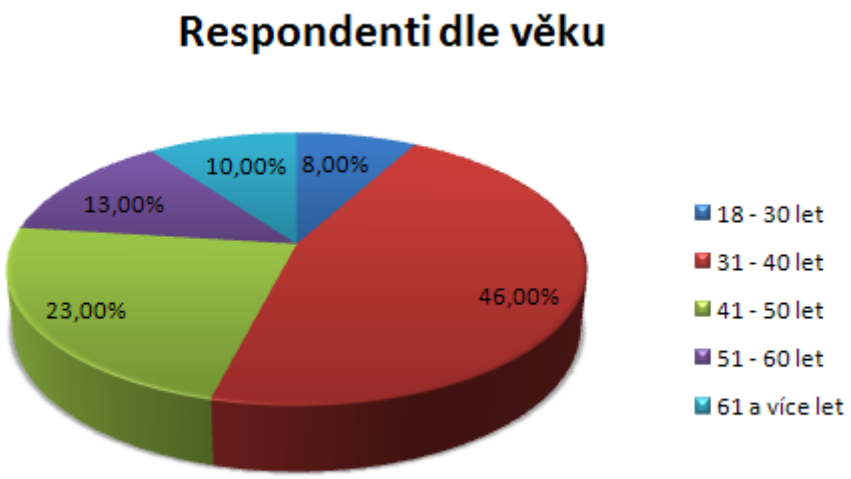
Respondenti dle vzdělání

Otázka číslo 13 v elektronickém dotazování týkající se dosaženého vzdělání dopadla zcela jasně. Ve 100 % případů respondenti označili dosažení vysokoškolského vzdělání a tedy obdržení vysokoškolského titulu.

Respondenti dle věku

Předposlední otázka dotazníku snažícího se odhalit praktické problémy elektronického podpisu se zaměřila na otázku věku vybraných respondentů.

Nejpočetnější skupinu tvořili vybraní respondenti ve věku mezi 31 a 40 lety a to z celých 46 %. Dotázaní ve věku mezi 41 a 50 lety byli druhou velmi početnou skupinou a tvořili 23 % celkového počtu respondentů. Ti oslovení mezi 51 a 60 lety byli třetí velkou skupinou a jejich hodnota v procentuálním vyjádření dosahovala 13 %. Skupina 61 a více let, tedy převážně respondenti v důchodovém věku, kteří se dotazování ochotně zúčastnili, zaujímali 10 % z celkového počtu. Poslední skupinu tvořili ti oslovení mezi 18 a 30 lety a to celých 8 %.

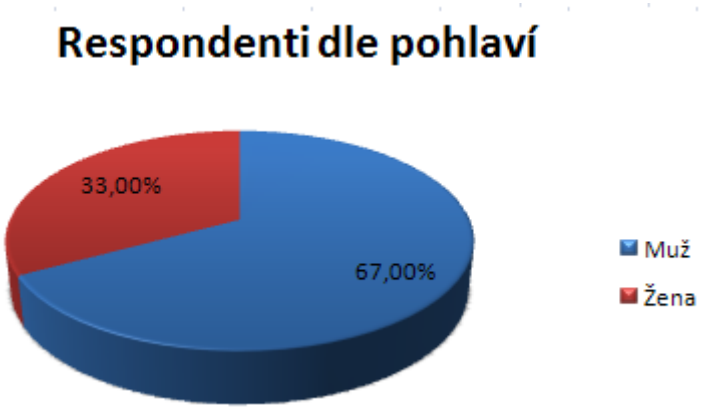


Graf 11: Respondenti dle věku Zdroj: vlastní

Respondenti dle pohlaví

Poslední otázkou výzkumu na zjištění praktických problémů elektronického podpisu byla otázka pohlaví vybraných respondentů. Výsledkem této otázky byla jasná převaha mužů nad ženami v to tak, že muži odpovídali v 67 % případů a ženy se zúčastnily logicky ve zbylých 33 %.

Výsledek lze podložit také statistikou Českého statistického úřadu, který na svých webových stránkách zveřejnil výsledky šetření zaměřujícího se na odhalení počtu mužů a žen v jednotlivých klasifikacích ekonomických činností, známých pod zkratkou CZ-NACE. Z tohoto vyplývá, že v roce 2010 bylo ve skupině M (profesní, vědecké a technické činnosti) zaměstnáno 14 tisíc mužů a pouhých 6,8 tisíc žen. Podrobnou tabulku s odvětvími činností zaměstnaných v NH lze nalézt v příloze této diplomové práce s vyznačením zmiňované skupiny M a jejího počtu zaměstnaných mužů a žen.



Graf 12: Respondenti dle pohlaví Zdroj: vlastní

4.7 Návrhy a doporučení

V následující kapitole budou nastíněny návrhy a doporučení, které logicky vyplynuly z elektronického dotazníkového šetření mezi vybranými respondenty. Nejčastěji uváděné praktické problémy se zřizováním a používáním elektronického podpisu budou zakomponovány do následujících návrhů a budou brány jako východisko pro zlepšení a zkvalitnění služeb elektronického podpisu jako takového.

Dle analýzy, která se zabývala odhalením praktických problémů elektronického podpisu, bylo zjištěno nejfrekventovanější místo sloužící pro zřízení elektronického podpisu. Stala se jím Česká pošta a domnívám se, že logické vysvětlení tkví v počtu poboček, které Česká pošta v České republice má a také z důvodu ceny pořízení jednotlivých certifikátů, ať již pro osobní či pracovní účely. Česká pošta je sice „nejoblíbenějším" zřizovatelem elektronického podpisu u respondentů v dotazníkovém šetření, ale smlouvy, které musí potencionální zřizovatelé vyplňovat, jsou do jisté míry zbytečně složité a také pro mnoho lidí nesrozumitelné. Proto navrhuji smlouvy co nejvíce zjednodušit a tím také usnadnit zřízení tohoto podpisu veřejností.

Dalším nedostatkem je pořizovací cena, která jak jsem již uvedla v předcházejících kapitolách, je značně odlišná u jednotlivých certifikačních autorit. Proto bych doporučila co nejvíce sjednotit ceny těchto poskytovaných certifikátů a také zavést výhody pro stálé klienty certifikačních autorit. Domnívám se, že značným „lákadlem" pro mnoho klientů by byly slevy u procesu prodloužení platnosti certifikátů. Pokud by si například klient prodlužoval již podruhé svůj certifikát u téže autority, dostal by na něj 50 % slevu.

Analýza praktických problémů elektronického podpisu také zkoumala, do jaké míry je elektronický podpis známý u široké veřejnosti. Odpovědi byly jednoznačné. Lidem elektronický podpis ve velké míře není znám a bylo by tedy vhodné odpovídajícím způsobem veřejnost o tomto druhu podpisu informovat. Příkladem mohou být letáky vydané jednotlivými certifikačními autoritami na pobočkách, podrobnými informacemi na internetových stránkách s nejrůznějšími odpovídajícími odkazy, aby poskytnuté informace byly kompletní a v neposlední řadě školení pořádané certifikačními autoritami pro své zaměstnance s pravidelnými opakováními.

Všeobecným nedostatkem, který vyplynul z několika odpovědí v dotazníkovém šetření, je bezpečnost elektronického podpisu. Respondenti se domnívají, že služby tohoto druhu podpisu nejsou odpovídajícím způsobem zabezpečeny. Proto navrhuji vyvinout co

možná nejbezpečnější antivirový program, který by data předávané elektronickou cestou ochránil. Jednotlivé certifikační autority, jakožto i státní správa, používají velmi kvalitní antivirové programy a disponují také svými odděleními, které se starají o bezpečnost dat. Jiná situace je ovšem u běžných uživatelů (fyzických osob), kteří si například zřizují elektronický podpis z domova a ve většině případů si antivirové programy pro své počítače stahují zdarma z internetu, jejich programy nejsou aktualizovány či tyto programy zcela postrádají a spoléhají na to, že právě oni se nemohou stát obětí „pirátů."

V neposlední řadě dalším problémem, který se objevoval, byla archivace elektronicky podepsaných dokumentů. U písemností, které disponují vlastnoručním podpisem, je situace velmi snadná. Opačná je u elektronických dokumentů, u kterých je archivace značným problémem, který souvisí s velmi dynamickým rozvojem v oblasti IT. Proto u tohoto nedostatku navrhuji zavést jednotný způsob archivace elektronických dokumentů a také speciální programy, které by jednoduše měnily staré datové formáty na nové bez možnosti ztráty dat obsažených v jednotlivých dokumentech.

Předposledním častým problémem je uznání elektronicky podepsaných písemností soudem či orgány činnými v trestním řízení. V tomto případě bych navrhovala vždy přizvání nezávislého a objektivního odborníka, který by v nejasných nebo složitých případech poskytoval rady a doporučení ohledně problematiky elektronického podpisu.

Posledním nedostatkem, který respondenty trápil, byla mezinárodní uznatelnost elektronického podpisu. Zde bych spatřovala řešení v jednotné legislativní úpravě tohoto podpisu napříč EU. Tímto by samozřejmě došlo ke shodnému vnímání elektronického podpisu v jednotlivých členských zemích a lidem by poté nevznikaly problémy se zřízením, uznatelností či prodlužováním svých podpisů v elektronické podobě.

5. Závěr

Diplomová práce byla koncipována takovými způsoby, aby co nejpřesněji a zároveň velmi kvalitně postihla pojem elektronického podpisu se zaměřením na jeho praktické využití a s tím související také velmi zřejmé a ve společnosti mnohonásobně diskutované praktické nedostatky. Cílem této práce bylo odkrytí problémů elektronického podpisu jako takového a dokumentů obsahujících tento podpis. Následně pomocí metody elektronického dotazování byly zjišťovány konkrétní nedostatky z pohledu jednotlivých respondentů vybraných pro tuto analýzu. Domnívám se, že cíl práce, stanovený v úvodu, byl splněn.

Práce, jak jsem již v samotném úvodu uvedla, byla koncipována do celkem pěti částí, které na sebe logicky navazují. Po úvodní kapitole jsem věnovala pečlivou pozornost teoretickým východiskům, kde jsem se čtenáři snažila co možná nejpřesněji přiblížit základní problematiku elektronického podpisu. Mimo zmiňovaný elektronický podpis jsem se zaměřila na objasnění skutečnosti certifikačních autorit, jednotlivých druhů certifikátů, které jsou poskytovány právě těmito autoritami, dále pojem časového razítka, elektronické značky a neopomněla jsem upozornit na výhody, nevýhody či bezpečnost elektronického podpisu v praxi.

Náplní třetí kapitoly byla právní úprava elektronického podpisu, jak z pohledu českého, tak také unijního práva. Zde byl klíčový zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů. Dále jsem zmínila jediné nařízení vlády a samozřejmě také nejrůznější vyhlášky, které se skutečnosti elektronického podpisu týkají. Z pohledu unijního práva jsem uvedla Směrnici 1999/93/EC Evropského parlamentu a Rady, o zásadách společenství pro elektronické podpisy. Tato Směrnice byla v práci podrobně rozepsána.

Nejdůležitější kapitolou byla čtvrtá kapitola, jejíž náplní se staly praktické problémy elektronického podpisu a následná analýza, jejímž úkolem bylo odhalit nedostatky tohoto podpisu a navrhnout možná opatření k jejich eliminaci. Analýza byla provedena pomocí elektronického dotazníkového šetření a vybrané skupiny respondentů, kteří odpovídali na předem určených 15 otázek. Jejich odpovědi byly následně zpracovány pomocí programu Microsoft Excel a vyhodnoceny jak slovně, tak pomocí grafického aparátu. Pomocí grafické metody byly výsledky analýzy jasně dané a srozumitelné. Výsledky tohoto dotazníkového šetření nadále sloužily pro možné návrhy a doporučení, jakým způsobem lépe prezentovat

problematiku elektronického podpisu, zdůraznit jeho výhody a zaměřit se na jeho bezpečné používání, nejen pro pracovní, ale také osobní účely.

Jak dokazují výsledky prováděného výzkumu, velká řádka respondentů je přesvědčena, že elektronický podpis jako takový není bezpečný a jeho povědomí u veřejnosti je velmi slabé. Oslovení uváděli také nedostatky v oblasti samotného zřízení, tedy složitou agendu, dále v platnosti certifikátu pouze na 365 dní a v neposlední řadě je znepokojovala oblast archivace elektronicky podepsaných dokumentů a viděli velké nedostatky v mezinárodní uznatelnosti elektronického podpisu, nejen napříč Evropskou unií, ale celosvětově.

Z výsledku analýzy praktických problémů elektronického podpisu je patrné, že existuje celá řada oblastí, kde je opravdu co zlepšovat a nesmíme opomíjet „klienty“ využívajících služeb elektronického podpisu, protože jsou to právě oni, kteří mohou být, a ve většině případů jsou, iniciátory změn vedoucích ke zkvalitnění vlastnoručního podpisu v elektronické podobě.

Závěrem je nutné shrnout zjištění a návrhy doporučované v rámci této práce. Nejčastěji zmiňovanými nedostatky, které se v průběhu elektronického dotazníkového šetření objevovaly byla odlišná pořizovací cena certifikátů u jednotlivých certifikačních autorit, dále složitá administrativa při zřizování podpisu, nedostatečná informovanost o této službě u veřejnosti, zabezpečení elektronického podpisu, archivace takto podepsaných dokumentů, uznání listin opatřených elektronickým podpisem soudy a v neposlední řadě jeho uznatelnost, nejen v rámci EU, ale také celosvětově.

Návrhy, které byly vyvozeny z odhalených nedostatků se týkaly zejména zjednodušení administrativy při zřizování podpisu, slevy při opakovaném prodlužování certifikátu u jedné certifikační autority, kvalitní antivirový program k řádnému zabezpečení služeb, které elektronický podpis nabízí. Dále například jednotný způsob archivace, přítomnost nezávislého experta u soudů či orgánů činných v trestním řízení a jednotná legislativní úprava elektronického podpisu zajišťující uznatelnost napříč EU i v celém světě.

Seznam použité literatury:

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

[2] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi: certifikáty a certifikační autority, legislativní rámec elektronického podpisu, praktické aplikace*. 1. vyd. Olomouc: ANAG, 2008. 157 s. ISBN 978-80-7263-465-1.

[3] DONÁT, J. Omyl z papíru. *Ekonom*, 2005, roč. 49, č. 6, s. 48 - 51. ISSN 1210-0714.

[4] DUŠKOVÁ-JANOUCHOVÁ, K. Firmy spíše důvěřují papíru. *PROFIT*, 2006, roč. 17, č. 25, s. 30 - 31. ISSN 1212-3498

[5] MACKOVÁ, A.; ŠTĚDROŇ, B. *Zákon o elektronických úkonech a autorizované konverzi dokumentů s komentářem.* 1. vyd. Praha: Wolters Kluwer ČR, 2009. 528 s. ISBN 978-80-7357-472-7.

[6] KOZEL, R. *Moderní marketingový výzkum: nové trendy, kvantitativní a kvalitativní metody a techniky, průběh a organizace, aplikace v praxi, přínosy a možnosti*. 1. vyd. Praha: Grada Publishing, 2006. 277 s. ISBN 80-247-0966-X

[7] PETERKA, J. *Báječný svět elektronického podpisu*. 1. vyd. Praha: CZ.NIC, 2011. 430 s. ISBN 978-80-904248-3-8.

[8] POLČÁK, R. Praxe elektronických dokumentů. *Bulletin advokacie*, 2011, 4. 7-8, s. 58 – 60. ISSN 1210-6348

[9] PRACHAŘ, J. *Obchodování přes internet.* 1. vyd. Kunovice: Evropský polytechnický institut, 2007. 64 s. ISBN 978-80-7314-117-2.

[10] ŠMÍD, D. Jak využívat elektronický podpis. *Sondy*, 2006, roč. 16, č. 35, s. 7. ISSN 0322-8800

[11] ZADRAŽIL, L. Zařiďme si přes internet. *Týden*, 2006. roč. 13, č. 41. s. 100-103. ISSN 1210-9940.

[12] ZELENKA, J. a kol. Ochrana dat: kryptologie. 1. vyd. Hradec Králové: Gaudeamus, 2003. 198 s. ISBN 80-7041-737-4.

Právní předpisy

[13] Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů

[14] Směrnice 1999/93/EC Evropského parlamentu a Rady o zásadách společenství pro elektronické podpisy

[15] Vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb

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

[17] Zákon č. 40/1964 Sb., občanský zákoník

[18] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů

Internetové zdroje

[19] BUSINESSCENTER. Zákon o elektronickém podpisu [online]. 2010 [cit. 2012-01-25]. Dostupný z WWW.:< http://business.center.cz/business/pravo/zakony/epodpis/>

[20] BUSINESSINFO. Elektronický podpis a jeho využití [online]. 2002 [2012-01-19]. Dostupný z WWW.:< http://www.businessinfo.cz/cz/clanek/podnikatelske-prostredi/elektronicky-podpis-a-jeho-vyuziti/1001234/2984/>

[21] BUSINESSINFO. Směrnice 1999/93/EC Evropského parlamentu a Rady o zásadách společenství pro elektronické podpisy [online]. 2002 [cit. 2012-01-26]. Dostupný z WWW.:< http://www.businessinfo.cz/files/file2122.pdf>

[22] ČESKÁ POŠTA*, s.p.* Kvalifikovaná certifikační autorita [online]. 2011 [cit. 2011-11-12]. Dostupný z WWW:< http://www.ceskaposta.cz/cz/sluzby/e-sluzby/kvalifikovana-certifikacni-autorita-id287/>

[23] ČESKÝ STATISTICKÝ ÚŘAD. Podíl podniků s webovými stránkami. [online]. 2012 [cit. 2012-01-25]. Dostupný z WWW:< http://www.czso.cz/csu/katalog.nsf/hledat?SearchView&count=20&searchorder=1&searchfuzzy=1&query=%28%28pod%EDl%20podnik%u016F%20s%20webov%FDmi%20str%E1nkami%29%29&database=all&kraje=all&skupiny=all&start=1>

[24] DIGITÁLNÍ PODPIS. Časové razítko [online]. 2010 [cit. 2011-11-13]. Dostupný z WWW.:< http://www.digitalni-podpis.cz/casove-razitko>

[25] DIGITÁLNÍ PODPIS. Slovník vybraných pojmů [online]. 2010 [cit. 2011-11-13]. Dostupný z WWW.:< http://www.digitalni-podpis.cz/slovnik-pojmu>

[26] EIDENTITY, a. s. O společnosti [online]. 2011 [cit. 2011-11-13]. Dostupný z WWW:< http://www.eidentity.cz/About.html >

[27] KLIMÁNKOVÁ, G. Elektronický podpis zdražil. Tip, jak za něj neplatit. *Měšec* [online]. 2010. [cit. 2012-02-15]. Dostupný z WWW: <http://www.mesec.cz/clanky/elektronicky-podpis-zdrazil-tip-jak-za-nej-neplatit/>.

[28] LORENC, M. Druhy elektronických podpisů. *Informační systém veřejné správy* [online]. 2007 [cit. 2011-11-03]. Dostupný z WWW:
< http://www.isvs.cz/e-podpis-podatelny/druhy-elektronickych-podpisu-5-dil.html>

[29] LORENC, M. Papírový versus elektronický dokument. Informační systém veřejné správy. [online]. 2007 [cit. 2012-01-19]. Dostupný z WWW:< http://www.isvs.cz/e-podpis-podatelny/papirovy-versus-elektronicky-dokument-27-dil.html>

[30] MĚŠEC.CZ. Pořiďte si už konečně elektronický podpis [online]. 2006 [cit. 2012-03-01]. Dostupný z WWW.:< http://www.mesec.cz/pr-clanky/poridte-si-uz-konecne-elektronicky-podpis/>

[31] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Bezpečnost elektronického podpisu a internetové bankovnictví [online]. 2010 [cit. 2012-02-02]. Dostupný z WWW.:< http://www.mvcr.cz/clanek/bezpecnost-elektronickeho-podpisu-a-internetove-bankovnictvi.aspx>

[32] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Přehled kvalifikovaných poskytovatelů a jejich kvalifikovaných služeb [online]. 2011 [cit. 2011-11-04]. Dostupný z WWW:< http://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb.aspx>

[33] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu [online]. 2010 [cit. 2012-01-31]. Dostupný z WWW.:< http://www.mvcr.cz/clanek/narizeni-vlady-c-495-2004-sb-kterym-se-provadi-zakon-c-227-2000-sb-o-elektronickem-podpisu-a-o-zmene-nekterych-dalsich-zakonu.aspx>

[34] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Příručka o elektronickém podpisu [online]. 2007 [cit. 2011-11-04]. Dostupný z WWW:
< http://aplikace.mvcr.cz/archiv2008/micr/files/3908/prirucka_el_podpis.pdf>

[35] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb [online]. 2010 [cit. 2012-01-26]. Dostupný z WWW.:< http://www.mvcr.cz/clanek/vyhlaska-c-378-2006-sb-o-postupech-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb.aspx>

[36] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Vyhláška č. 496/2004 Sb., o elektronických podatelnách [online]. 2010 [cit. 2012-01-26]. Dostupný z WWW.:< http://www.mvcr.cz/clanek/vyhlaska-c-496-2004-sb-k-elektronickym-podatelnam.aspx>

[37] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Zákon č. 227/200 Sb., o elektronickém podpisu [online]. 2010 [cit. 2012-01-25]. Dostupný z WWW.:< http://www.mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx>

[38] PODNIKATEL. Zákon č. 40/1964 Sb., občanský zákoník [online]. 2010 [cit. 2012-01-31]. Dostupný z WWW.:< http://www.podnikatel.cz/zakony/zakon-c-40-1964-sb-obcansky-zakonik/>

[39] PRVNÍ CERTIFIKAČNÍ AUTORITA, a. s. O nás [online]. 2011 [cit. 2011-11-12]. Dostupný z WWW:< http://www.ica.cz/O-nas.aspx>

[40] ZÁKONY-ONLINE. Zákon o elektronickém podpisu [online]. 2005 [cit. 2012-01-25]. Dostupný z WWW:< http://zakony-online.cz/?s57&q57=6>

Seznam použitých zkratek

apod.	a podobně
a.s.	akciová společnost
CA	certifikační autorita
CZ – NACE	Klasifikace ekonomických činností
č.	číslo
ČR	Česká republika
DPH	daň z přidané hodnoty
EC	European Commission
EU	Evropská unie
IT	Information technology
např.	například
OSSZ	Okresní správa sociálního zabezpečení
OSVČ	osoba samostatně výdělečně činná
PSC	poskytovatelé certifikačních služeb
resp.	Respektive
Sb.	Sbírka
s.p.	státní podnik
tj.	to je
tzv.	takzvaný
ZoEP	zákon o elektronickém podpisu

Prohlášení o využití výsledků diplomové práce

Prohlašuji, že

- jsem byla seznámena s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně ke své vnitřní potřebě, diplomovou práci užít (§ 35 odst. 3);
- souhlasím s tím, že diplomová práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího diplomové práce. Souhlasím s tím, že bibliografické údaje o diplomové práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, diplomovou práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne 27. 4. 2012

……...

Petra Šmídová

Adresa trvalého pobytu studenta:

N. Frýda 153/14

700 30 Ostrava – Dubina

Seznam příloh

Příloha 1: Dotazník

Vážený respondente, Vážená respondentko,

jsem studentkou 5. ročníku Ekonomické fakulty VŠB – TUO, oboru Ekonomika a právo v podnikání. Cílem mé diplomové práce je analyzovat problémy elektronického podpisu v praxi. Chtěla bych Vás touto cestou požádat o vyplnění následujícího krátkého dotazníku.

Tento dotazník je zcela anonymní a všechny Vámi poskytnuté údaje budou sloužit pouze pro potřebu diplomové práce. **Není – li stanoveno jinak, označte prosím jen jednu odpověď.** Děkuji za Váš čas a ochotu dotazník vyplnit.

Bc. Petra Šmídová

1. Máte zřízen elektronický podpis? (pokud ne, přejděte prosím na otázku č.8)
   - ☐ Ano
   - ☐ Ne

2. Proč jste si zřídili elektronický podpis? (např. použití v pracovním či osobním životě)

   ……

3. Kde jste si jej založili?
   - ☐ Banka
   - ☐ Česká pošta
   - ☐ Internet
   - ☐ První certifikační autorita
   - ☐ jinak (rozepište, prosím)……..

4. Jak dlouho již využíváte služeb elektronického podpisu?
   - ☐ méně než 1 rok
   - ☐ 1-5 let
   - ☐ více než 5 let

5. Označte, jaké problémy máte nebo jste měli se zřízením elektronického podpisu? (možnost označit i více odpovědí)
   - ☐ Složitá administrativa při zřizování
   - ☐ Cena pořízení
   - ☐ Dostupnost počítače a internetového připojení
   - ☐ Neschopnost pokročilejší práce s počítačem a internetem
   - ☐ Nedostatečné množství informací o elektronickém podpisu
   - ☐ Neuspokojivé vysvětlení použitelnosti elektronického podpisu v praxi
   - ☐ jiné (uveďte, prosím)……..

6. Označte, jaké problémy máte nebo jste měli s používáním elektronického podpisu? (možnost označit i více odpovědí)

☐ Archivace dokumentů opatřených elektronickým podpisem
☐ Průkaznost provedené operace (např. potvrzení o předání dokumentů)
☐ Mezinárodní uznatelnost elektronického podpisu
☐ Bezpečnost elektronického podpisu
☐ jiné (uveďte, prosím)…….

7. Jaký konkrétní problém jste měli Vy s elektronickým podpisem v praxi? (rozepište)

…….

8. Ohodnoťte, jaké problémy jsou dle Vašeho názoru nejvíce závažné? (1-velký problém, 5-žádný problém)

	1	**2**	**3**	**4**	**5**
Bezpečnost	☐	☐	☐	☐	☐
Průkaznost	☐	☐	☐	☐	☐
Uznatelnost	☐	☐	☐	☐	☐
Archivace	☐	☐	☐	☐	☐
Neinformovanost	☐	☐	☐	☐	☐

9. Myslíte si, že je elektronický podpis dostatečně bezpečný?

☐ Ano
☐ Ne

10. Domníváte se, že široká veřejnost zná pojem elektronického podpisu a jeho funkce?

☐ Ano
☐ Ne

11. Jste:

☐ Student
☐ Podnikatel
☐ Zaměstnance
☐ Důchodce
☐ Mateřská dovolená
☐ Nezaměstnaný/á

12. Kde konkrétně pracujete? (rozepište, např. název společnosti a obor)

……..…….

13. Jaké je Vaše nejvyšší ukončené vzdělání?

- ☐ Základní
- ☐ Střední bez maturity
- ☐ Střední s maturitou
- ☐ Vyšší odborné
- ☐ Vysokoškolské

14. Jaký je Váš věk?

- ☐ 18 – 30 let
- ☐ 31 - 40 let
- ☐ 41 – 50 let
- ☐ 51 - 60 let
- ☐ 61 a více let

15. Jste:

- ☐ Muž
- ☐ Žena

Příloha 2: Podniky v ČR s webovými stránkami

%

	2006	2007	2008
Celkem	**70,1**	**71,2**	**74,0**
podle velikosti podniku			
malé (10–49 zaměstnanců)	66,1	67,5	70,3
střední (50–249 zaměstnanců)	83,6	83,7	85,8
velké (250 a více zaměstnanců)	91,9	91,7	92,9
podle ekonomické činn. podniku			
Zpracovatelský průmysl	68,8	71,8	74,0
Výroba a rozvod elektřiny, plynu a vody	64,2	62,3	67,3
Stavebnictví	71,0	62,1	66,9
Prodej a oprava motorových vozidel	74,4	73,4	74,6
Velkoobchod	82,9	86,6	86,1
Maloobchod	53,7	55,4	66,4
Ubytování	90,1	91,9	92,6
Doprava a skladování	61,3	59,3	54,9
Pošta a telekomunikace	94,0	93,9	95,5
Peněžnictví a pojišťovnictví	85,7	91,8	89,3
Činnosti v oblasti nemovitostí; VaV	65,9	68,7	69,3
Činnosti v oblasti výpočetní techniky	94,4	95,6	94,3
Ostatní podnikatelské činnosti (1)	71,9	73,3	79,2
Audiovizuální činnosti	82,9	91,9	92,9
Kult., sport.a ostatní rekreační činnosti	70,7	78,3	78,2
Ostatní činnosti (2)	54,3	58,3	56,8
podle místa registrace podniku			
podniky registr. mimo hl. město Prahu	67,7	68,2	71,3
podniky registr. v hl. městě Praze	79,1	81,7	83,2

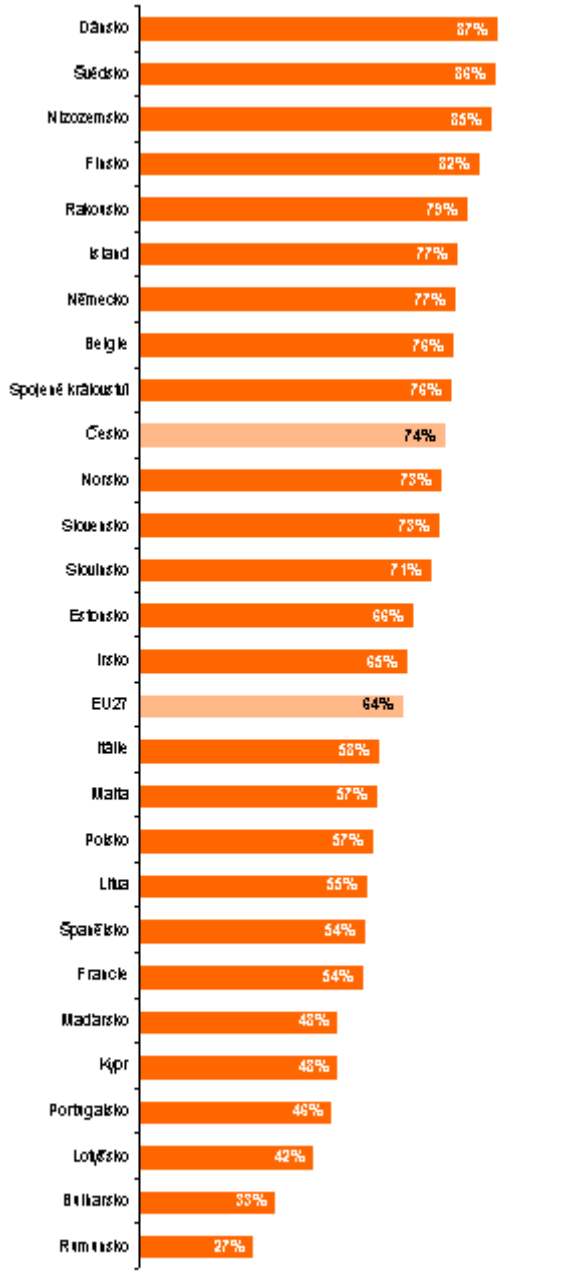
podíl z celk. počtu podniků v dané velikostní, odvětvové a regionální skupině

1) Právní, účetní, reklamní činn.; Průzkum trhu; Architekt. a inženýrské činn.

2) Kadeřnické, kosmetické a podobné služby; Praní a chemické čištění; atd.

Obrázek 1: Podniky v ČR s webovými stránkami Zdroj: [23]

Příloha 3: Podniky v Evropě s webovými stránkami

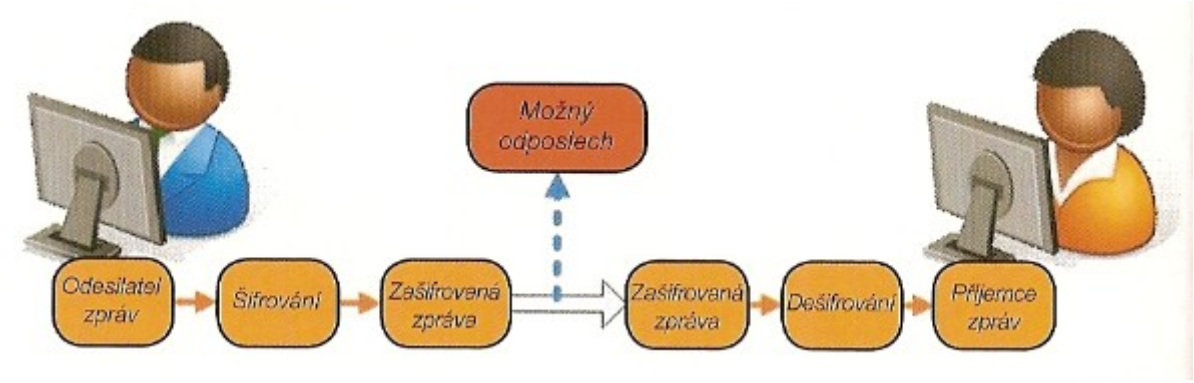


podíl na celkovém počtu podniků s 10 a více zaměstnanci

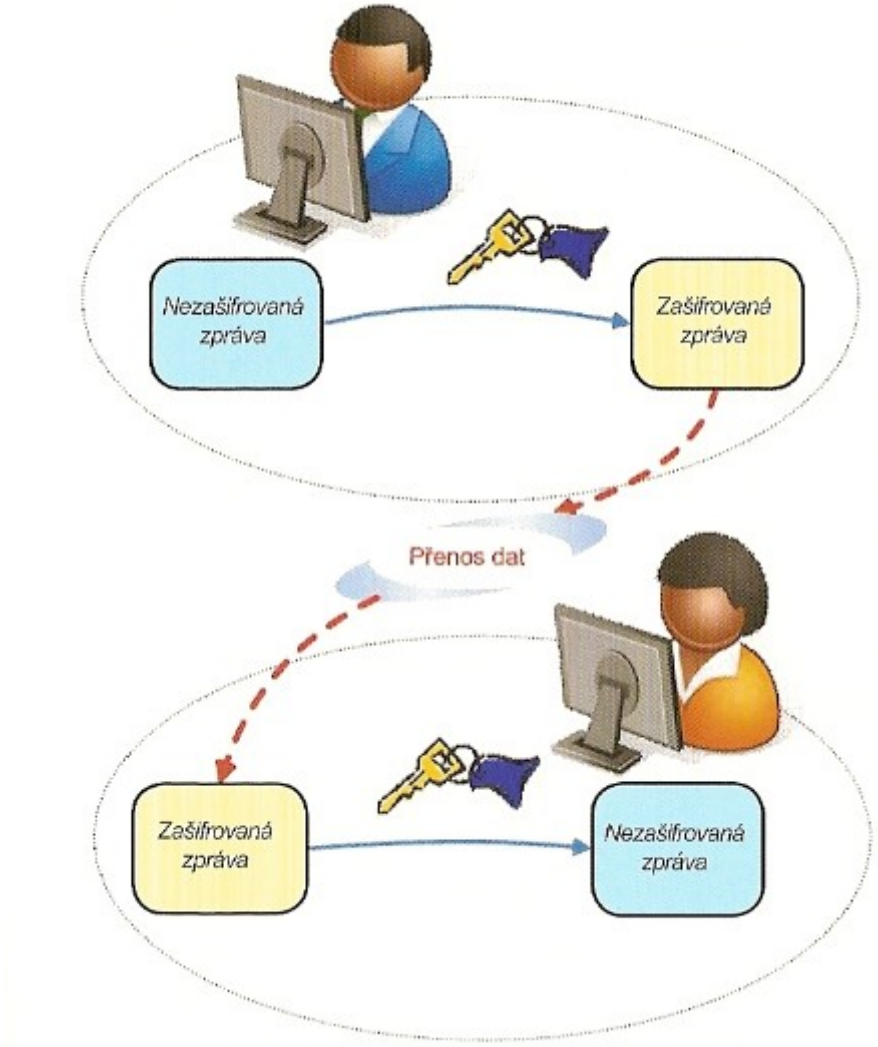
Zdroj: Eurostat, 2009

Obrázek 2: Podniky v ČR s webovými stránkami Zdroj: [23]

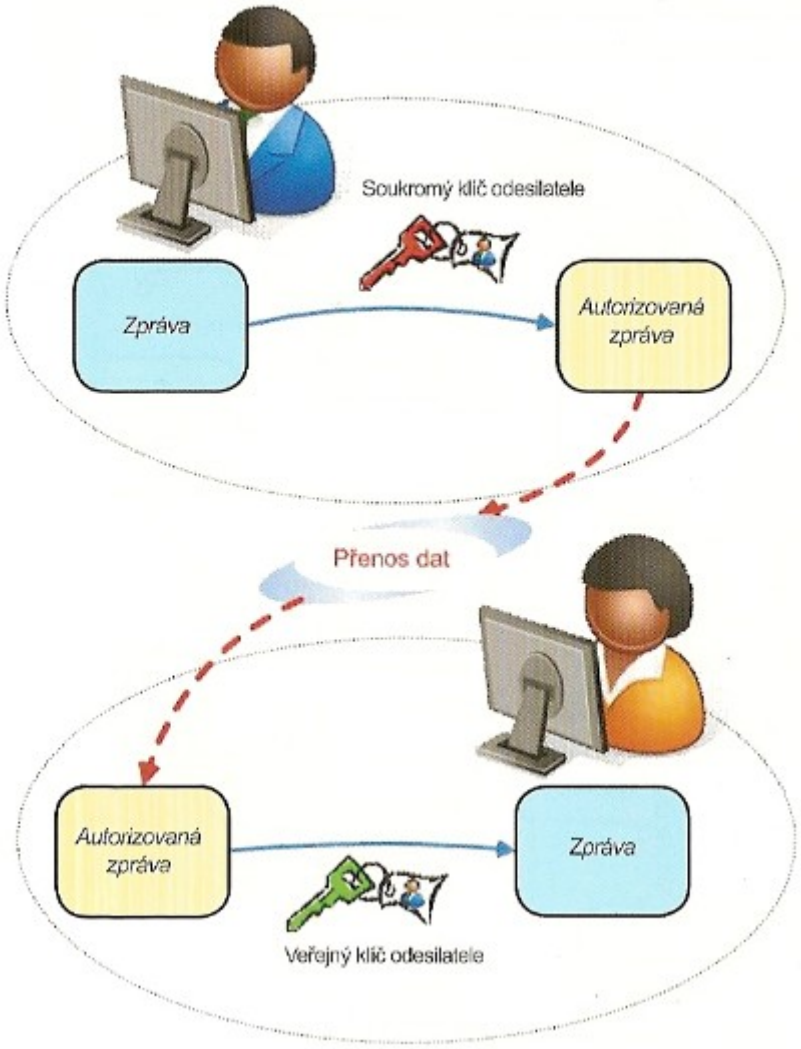
Příloha 4: Bezpečná komunikace – základy kryptografie



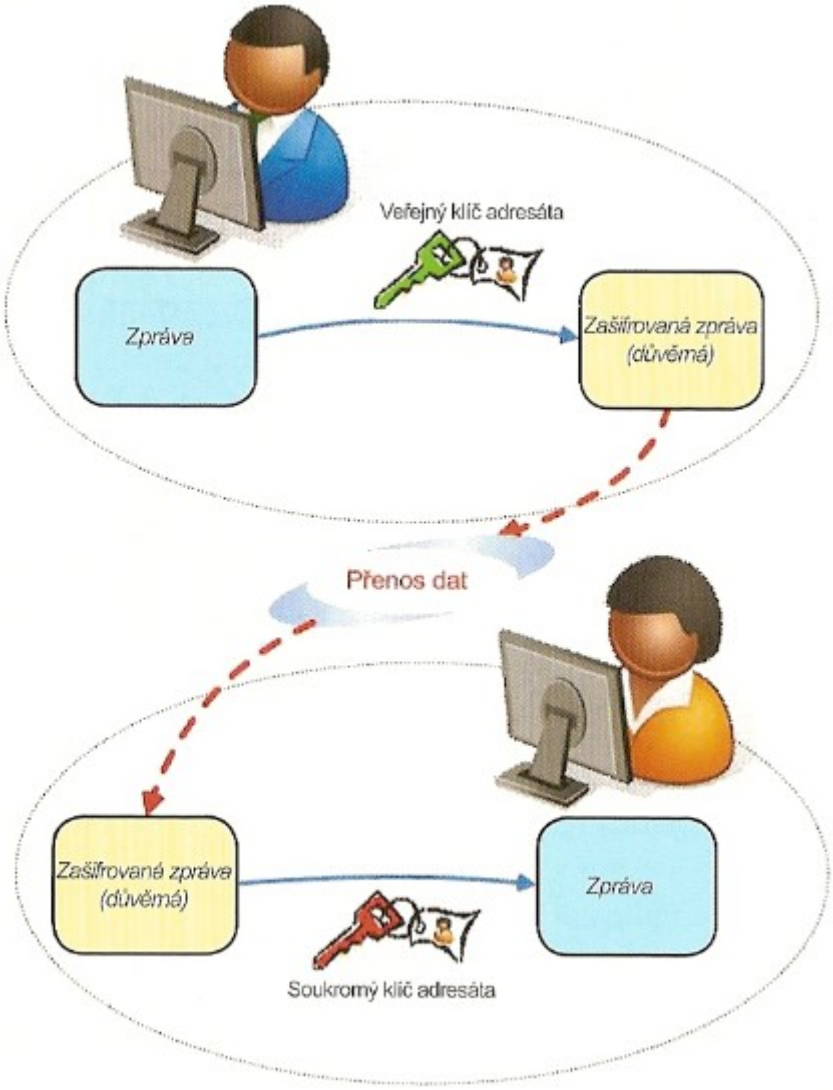
Obrázek 3: Přenos zprávy šifrovaným kanálem Zdroj: [2]



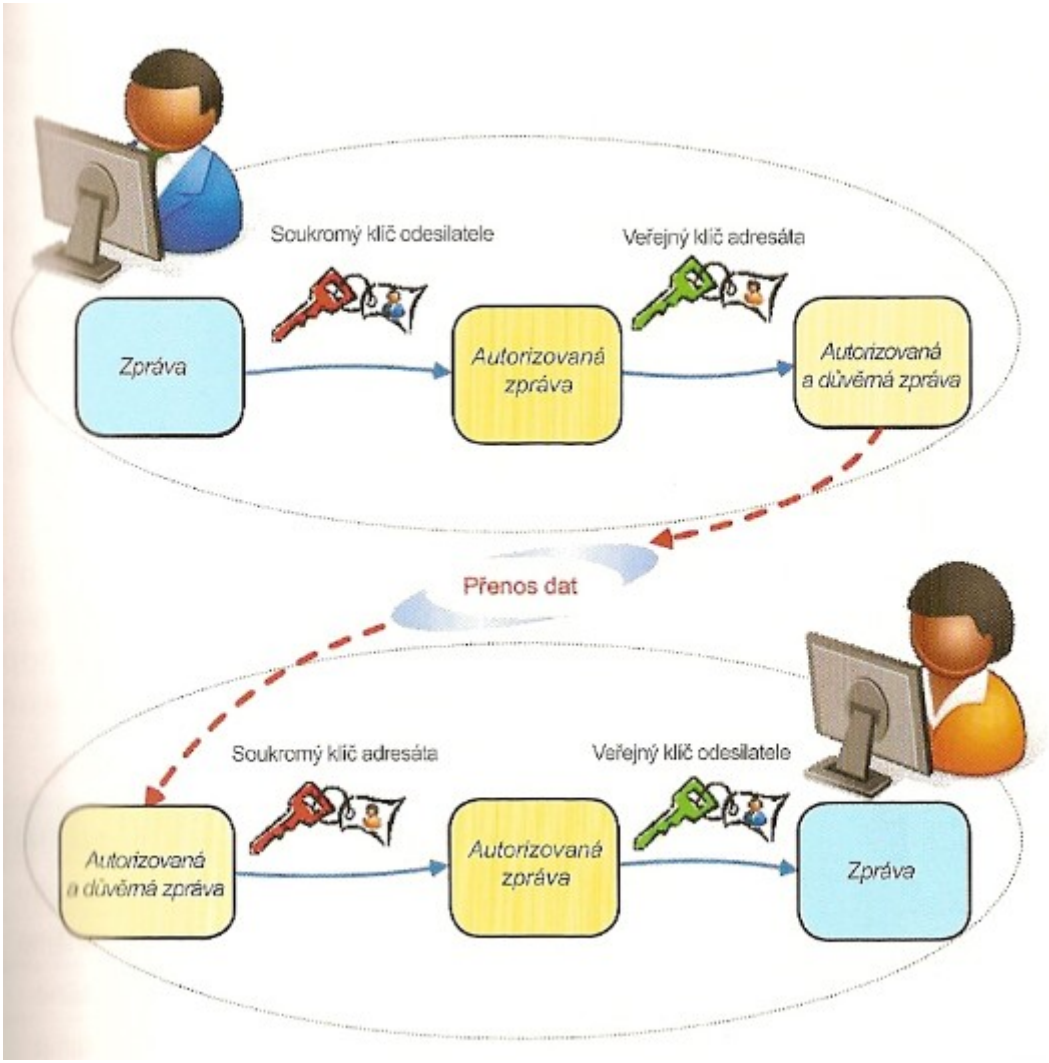
Obrázek 4: Šifrování zpráv symetrickou šifrou Zdroj: [2]



Obrázek 5: Přenos neadresované, nezašifrované (veřejné), ale autorizované zprávy Zdroj: [2]

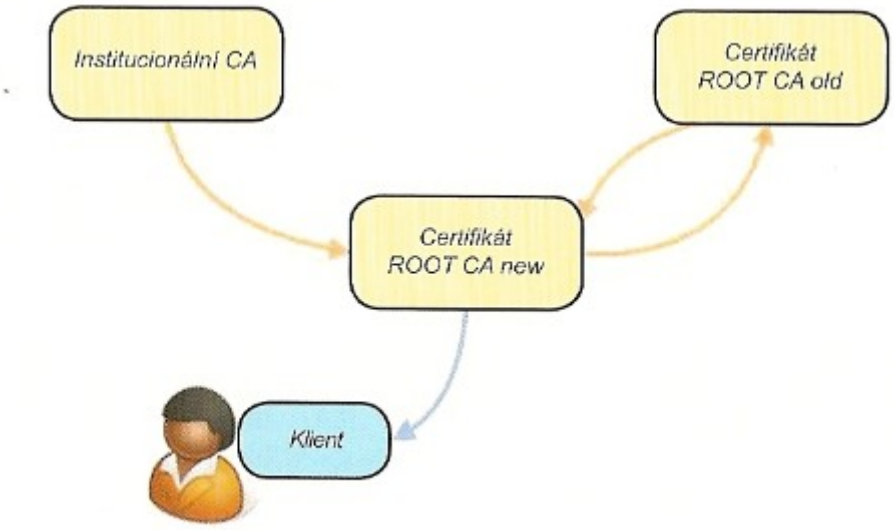


Obrázek 6: Přenos adresované, zašifrované (důvěrné), ale neautorizované zprávy Zdroj: [2]



Obrázek 7: Přenos adresované, zašifrované (důvěrné) a autorizované zprávy Zdroj: [2]

Příloha 5: Certifikáty



Obrázek 8: Řetězce důvěry I.CA. Zdroj: [2]