Možnosti využívání elektronického podpisu při komunikaci s orgány veřejné správy

Veronika Vlčková

Bakalářská práce
2008

Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky

Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky
Ústav veřejné správy a regionálního rozvoje
akademický rok: 2007/2008

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Veronika VLČKOVÁ**
Studijní program:	**B 6202 Hospodářská politika a správa**
Studijní obor:	**Veřejná správa a regionální rozvoj**
Téma práce:	**Možnosti využívání elektronického podpisu při komunikaci s orgány veřejné správy**

Zásady pro vypracování:

Úvod

I. Teoretická část

- **Na základě studia odborné literatury charakterizujte základní pojmy týkající se elektronického podpisu a elektronické podatelny.**

II. Praktická část

- **Proveďte dotazníkový průzkum využívání elektronického podpisu u elektronických podatelen v institucích veřejné správy Olomouckého kraje.**
- **Zhodnoťte výsledky získané dotazníkovým průzkumem o využívání elektronického podpisu u elektronických podatelen v Olomouckém kraji.**
- **Navrhněte doporučení k dalším možnostem využívání elektronického podpisu v institucích veřejné správy Olomouckého kraje.**

Závěr

Rozsah práce: **cca 40 stran**

Rozsah příloh:

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

Seznam odborné literatury:

[1] JAŠEK, R. Ochrana znalostí a dat v podnikových informačních systémech. 1. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2002. 115 s. ISBN 80-7318-095-2.
[2] ROSMAN, P. Informatika pro ekonomy. 2. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006. 233 s. ISBN 80-7318-430-3.
[3] BOSÁKOVÁ, D., KUČEROVÁ, A., PECA, P. 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.
[4] DOSTÁLEK, L., VOHNOUTOVÁ, M. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. 1. vyd. Brno: Computer Press, 2006.
534 s.ISBN 80-251-0828-7.
[5] RYBKA, M., MALÝ, O. Jak komunikovat elektronicky. 1. vyd. Praha: Grada Publishing, 2002. 92 s. ISBN 80-247-0208-8.

Vedoucí bakalářské práce: **Ing. Miroslava Dolejšová, Ph.D.**
Ústav informatiky a statistiky

Datum zadání bakalářské práce: **17. března 2008**

Termín odevzdání bakalářské práce: **23. května 2008**

Ve Zlíně dne 17. března 2008

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ Fakulta managementu a ekonomiky

doc. Dr. Ing. Drahomíra Pavelková
děkan

doc. RNDr. René Wokoun, CSc.
ředitel ústavu

ABSTRAKT

V bakalářské práci se zabývám možnostmi využívání elektronického podpisu při komunikaci s orgány veřejné správy Olomouckého kraje. V teoretické části uvádím základní informace o elektronickém podpisu, elektronické podatelně a dalších pojmech souvisejících s elektronickým podpisem a jeho právní úpravou. V praktické části analyzuji využívání elektronického podpisu ve veřejné správě, postoje a názory zaměstnanců veřejné správy na práci s elektronickým podpisem a elektronickými podatelnami.

Klíčová slova:

elektronický podpis, elektronická podatelna, šifrování, veřejný klíč, soukromý klíč, certifikát, veřejná správa, zákon o elektronickém podpisu, časové razítko.

ABSTRACT

In this bachelor thesis I deal with the possibilities of the utilization of the electronic signature at the communication with the public administration institutions in the Region of Olomouc. In the theoretical part I mention the basic information of the electronic signature, the electronic filing room and other expressions associated with the electronic signature and its legal regulations. In the practical part I analyze the utilization of the electronic signature in the public administration institutions, positions and opinions of the establishment of the public administration institutions on the work with the electronic signature and filing rooms.

Keywords:

electronic signature, electronic filing room, encryption, public key, private key, certificate, public administration, the law about electronic signature, clock stamp.

Ráda bych touto cestou poděkovala všem, kteří se zasloužili o vznik této bakalářské práce. Především bych chtěla poděkovat Ing. Miroslavě Dolejšové, Ph.D. za její odbornou pomoc a velkou ochotu řešit mé dotazy. Dále bych chtěla poděkovat zaměstnancům institucí veřejné správy Olomouckého kraje za poskytnutí veškerých informací potřebných pro vypracování této bakalářské práce, především pak děkuji za vyplnění dotazníků.

„Vzdělání je to jediné, co v nás zůstane po tom, co zapomeneme vše, co jsme se naučili ve škole!“

Albert Einstein

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

Ve Zlíně 22.5.2008 ……...

OBSAH

ÚVOD

Nacházíme se bez nadsázky v období elektronického věku. Před pár lety měl internet jen zlomek národa, dnes je zaveden do většiny našich domácností. Málokoho by nedávno napadlo, že bude moci řídit své bankovní operace nebo posílat formuláře a daňová přiznání elektronicky z tepla svého domova. Dnes se elektronická komunikace s orgány veřejné správy, ale i s jinými institucemi jako jsou banky, pojišťovny, stále více a více rozmáhá.

Také životní tempo lidí je rychlé a všichni se proto snažíme si jakýmkoliv způsobem v této hektické době ušetřit trochu času, který bychom mohli věnovat své rodině. Usnadněním nám může být již zmiňovaná elektronická komunikace s veřejnou správou. Je mnohem pohodlnější podat například daňové přiznání elektronicky z domu, bez stresu ve frontách na finančním úřadě. Elektronický podpis nás identifikuje stejně jako náš vlastnoruční podpis a přitom nemusíme nikam chodit.

V bakalářské práci se zaměřím na možnosti využívání elektronického podpisu při komunikaci s orgány veřejné správy, koneckonců tak již název napovídá, konkrétně pak na komunikaci s orgány veřejné správy Olomouckého kraje.

Jako účinný ukazatel pro hodnocení možností využívání elektronického podpisu jsem zvolila dotazník, který obsahuje 13 otázek a který byl směřován zaměstnancům institucí veřejné správy Olomouckého kraje. Dotázaní zde měli i prostor k vyjádření vlastních názorů a námětů na zlepšení v oblasti využívání elektronického podpisu a elektronických podatelen. Hlavním cílem tohoto dotazníku bylo navrhnout doporučení ke zvýšení využitelnosti elektronického podpisu v institucích veřejné správy Olomouckého kraje.

I. TEORETICKÁ ČÁST

1 CO JE TO ELEKTRONICKÝ PODPIS

Elektronický podpis je – stejně jako „ruční“ (vlastnoruční) podpis – výsledkem nějakého procesu, vyplývajícího z rozhodnutí podepisující osoby, jehož úkolem je stvrdit vůli této osoby, případně její identitu.

Vlastnoruční podpis je výsledkem uplatnění návyku psaní, získaného v podobě individuálního relativně stálého písemného projevu člověka. Vznik individuálnosti písma je důsledkem vytvoření dynamického stereotypu psaní, tedy vypracování složitého systému podmíněných indexů, které jsou závislé na stupni procvičování. Jak u podepisování, tak u zkoumání pravosti (ověřování) podpisu jde o procesy převážně subjektivního charakteru, u nichž se promítají obecné a individuální vlastnosti zúčastněných osob.

Elektronický podpis je naproti tomu od okamžiku podpisu, tedy od okamžiku učinění rozhodnutí podepisující osoby až po okamžik ověření pravosti podpisu, efektivním výsledkem technologického, na zvláštnostech zúčastněných osob nebo situace nezávislého, procesu. Je výsledkem aplikace určité, pro podepisující osobu charakteristické vlastnosti (tajné informace) na podepisovaný text.

Elektronický podpis je zpravidla chápán jako číslo, které vytváří podepisující osoba pomocí svých dat pro vytváření elektronického podpisu a pomocí zprávy, kterou podepisuje.

Podle zákona o elektronickém podpisu č. 486/2004 Sb., který je úplným zněním zákona č. 227/2000 Sb. o elektronickém podpisu a změně některých dalších zákonů, jak vyplývá ze změn provedených zákonem č. 226/2002 Sb., zákonem č. 517/2002 Sb. a zákonem č. 440/2004 Sb., se elektronickým podpisem rozumí 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. [1]

Jednoduše řečeno, elektronický podpis říká příjemci zprávy, že to, co vidí námi podepsané, je skutečné od nás – což je v dnešním anonymním světě internetu velmi cenné.

Teoreticky by se pod pojem „elektronický podpis“ vešel i podpis, který je napsán z klávesnice počítače. Takový podpis však příliš velkou důvěru nevzbuzuje – je těžké identifikovat a prokázat, kdo jej skutečně napsal. Elektronickým podpisem je tedy v praxi zpravidla míněn zaručený elektronický podpis. [2]

1.1 K čemu slouží elektronický podpis

Existuje mnoho možností využití elektronického podpisu, mezi nejčastější však patří komunikace občanů s veřejnou správou – elektronické podání žádostí (žádost o výpis z rejstříku trestu, žádost o živnostenský list) či podání daňových přiznání, nahrazování papírové dokumentace a papírové komunikace elektronickou nebo například elektronický obchod.

Nahrazování papírové dokumentace a papírové komunikace elektronickou je typické pro bankovnictví. Díky elektronickému bankovnímu výpisu či možnosti poslat platební příkaz elektronicky si spousta firem ušetří práci. Již nemusí opisovat částky z papírového výpisu do svých účetních systémů, stačí jim stáhnout si tento elektronický výpis, který se pomocí různých převodových můstků téměř zaúčtuje sám. Výhodou také je, že nemusí chodit s každým příkazem do banky, vše jde elektronickou cestou.

Elektronický podpis se dá využít všude tam, kde je dnes nutný vlastnoruční podpis. Všechny dokumenty lze převést z papírové podoby na dokumenty elektronické a všechny podpisy je možné převést na jejich elektronickou formu. Podepisovat i ověřovat podpisy lze takto srovnatelně rychleji a efektivněji. Je možné podepsat dokonce i to, co lze ručně opatřit podpisem jen velmi těžko – obsah diskety, fotografii, přístupy do databáze a mnoho dalších. [3]

1.2 Princip fungování elektronického podpisu

Elektronický podpis představuje nástroj, který umožňuje bezpečně a spolehlivě určit identitu dané osoby. Je založen na principu asymetrického šifrování. Samotný elektronický podpis vzniká tak, že se nejprve určí otisk podepisovaných dat (hash), který se následně zašifruje soukromým klíčem dané osoby. Ověření platnosti podpisu na druhé straně potom probíhá tak, že se porovná otisk dat z podpisu (dešifruje se pomocí veřejného klíče) s aktuálním otiskem daného souboru. Pokud jsou oba otisky stejné, podpis platí. Pokud se liší, je zřejmé, že podpis (zašifrovaný otisk) k daným datům nepatří, nebo že data byla po podpisu změněna. [4]

1.3 Digitální podpis

Metodou využívanou pro tvorbu a fungování elektronického podpisu je metoda digitálního podpisu, která využívá ke svému fungování dva klíče – veřejný a soukromý.

Digitální podpis je bezpečnostní mechanismus, který byl vytvořen jako ekvivalent našeho ručního podpisu pro použití v elektronické komunikaci. Ve standardní elektronické komunikaci neexistuje způsob, jak ověřit, zda-li je zdrojem dat skutečně ten, který je udán. Také není možné zjistit, zda-li informace v elektronické komunikaci nebyla při přenosu pozměněna, ani zabezpečit její odposlechnutí. [3]

Digitální podpis řeší tuto problematiku a je nedílnou součástí důvěryhodné a profesionální elektronické komunikace.

2 DRUHY ELEKTRONICKÝCH PODPISŮ

Český právní řád definuje různé typy elektronických podpisů. Ne každý typ elektronického podpisu můžeme považovat za důvěryhodný. Podle míry důvěryhodnosti, jakou jim přikládáme, rozlišujeme následující typy elektronických podpisů:

- elektronický podpis,
- zaručený elektronický podpis,
- zaručený elektronický podpis založený na certifikátu,
- zaručený elektronický podpis založený na kvalifikovaném certifikátu od akreditovaného poskytovatele služeb.

2.1 Elektronický podpis

Jedná se o podpis, který napíšeme například na konci emailové zprávy. Není však zaručeno, kdo je autorem tohoto podpisu. Je více než jasné, že takový podpis za nás může udělat kdokoliv, proto se jedná o důvěryhodnost téměř mizivou.

Tento podpis můžeme využívat například při korespondenci s rodinou, přáteli či kolegy v práci, kde neuvádíme žádná utajovaná data ani skutečnosti, které by měly být chráněny před ostatním světem.

2.2 Zaručený elektronický podpis

Existují tedy dva stupně elektronického podpisu, a to elektronický podpis „obyčejný“ a elektronický podpis „zaručený“. Jak už jsme si řekli, zákon o elektronickém podpisu říká, že (obyčejným) *elektronickým podpisem jsou údaje v elektronické podobě, které jsou připojené k datové právě nebo jsou s ní logicky spojené a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě.* [1]

Zákon však neříká nic o tom, jakou technologií mají být tato data vytvořena a jak se má postupovat při zmíněném ověření totožnosti. Proto existuje zaručený elektronický podpis,

u kterého se jedná o údaje, které jsou připojeny k obsahu elektronického dokumentu a které jsou vytvořeny zvláštním postupem s využitím kryptografických principů. [2]

Na rozdíl od „ obyčejného“ elektronického podpisu má zaručený elektronický podpis následující charakteristiky:

- fyzická osoba (podepisující osoba) , která zprávu podepsala, nemůže popřít, že je původcem této zprávy,
- je možné zjistit, zda zpráva nebyla změněna poté, co byla podepsána,
- je možné zjistit identitu podepsané osoby. [5]

Zaručeným elektronickým podpisem nelze zprávu elektronicky podepsat dřív, dokud není napsaná. Z toho vyplývá, že tento podpis nemůže existovat bez zprávy, která jím má být podepsána.

2.3 Zaručený elektronický podpis založený na certifikátu

Tento typ podpisu je základním typem elektronického podpisu, kterým se zabývá zákon o elektronickém podpisu. Slouží pro styk příjemce a jiného subjektu, který vlastní kvalifikovaný certifikát. Příjemce podepsanou osobu nemusí osobně znát, data pro ověřování elektronického podpisu získá příjemce z kvalifikovaného certifikátu. Právní jistota v souvislosti s tímto způsobem komunikace vyplývá ze zákona o elektronickém podpisu, nemusí se tedy na rozdíl od předchozího případu uzavírat speciální smlouvy pro právní podporu této komunikace. Důvěra v obsah certifikátu je podmíněna důvěrou v poskytovatele certifikačních služeb, který certifikát vydal. Tato důvěra vyplývá i ze skutečnosti, že zákon o elektronickém podpisu stanoví poskytovatelům vydávajícím kvalifikované certifikáty celou řadu povinností. [5]

Podpisu může být použito i k „anonymnímu“ styku (místo jména podepisující osoby může být v kvalifikovaném certifikátu uveden pseudonym, ovšem s označením, že se jedná o

pseudonym). V případě právního sporu může být „anonymní“ držitel certifikátu dohledán prostřednictvím údajů, které má k dispozici poskytovatel certifikačních služeb. Uvedený typ podpisu lze použít všude tam, kde se v zákoně o elektronickém podpisu umožňuje použít elektronický podpis. Profil tohoto podpisu je zpřísněn – nestačí, aby byl kvalifikovaný certifikát vydán poskytovatelem, který vydává kvalifikované certifikáty, ale poskytovatelem, který byl akreditován Úřadem pro ochranu osobních údajů. [5]

Obecně se považuje tento typ za vhodný pro přímou komunikaci mezi subjekty. Není vhodný k archivaci dat a tam, kde je nutné zpětně prokazovat, kdy přesně byl dokument podepsán.

2.4 Elektronický podpis založený na kvalifikovaném certifikátu od akreditovaného poskytovatele služeb

Jedná se o typ podpisu, který je vyžadován při komunikaci s veřejnou správou. Je podpisem nejvěrohodnějším.

Zatímco pro běžnou emailovou komunikaci lze využít jakéhokoliv z výše uvedených podpisů, pro styk s orgány veřejné správy je třeba použít podpis nejdůvěryhodnější – tedy zaručený elektronický podpis založený na kvalifikovaném certifikátu od akreditovaného poskytovatele certifikačních služeb. Pro využití elektronického podpisu například uvnitř firem bude plně postačující zaručený elektronický podpis založený na kvalifikovaném certifikátu. [5]

Typickým znakem elektronického podpisu založeného na kvalifikovaném certifikátu od akreditovaného poskytovatele služeb je to, že tento podpis je vždy spojen jen s jednou fyzickou osobou, přesněji řečeno, kvalifikovaný certifikát vydává akreditovaný poskytovatel certifikačních služeb fyzické osobě, která je odpovědná za podepsání každé ze zpráv tímto podpisem.

Kromě těchto typů elektronických podpisů se lze setkat s obdobnými názvy jako:

- Kvalifikovaný podpis – často je pod tímto pojmem míněn zaručený elektronický podpis.
- „Vylepšený“ elektronický podpis (advanced electronic signature) – elektronický podpis, který kromě svých základních funkcí poskytuje další funkce jako například možnost šifrování obsahu zprávy.
- Kvalifikovaný podpis určený pro archivaci dat (qualified electronic signature with long-term validity) – podpisy vhodné pro dlouhodobé skladování dat.
- Hromadný podpis (aggregate signature) – podpisové schéma, které umožňuje shlukování stávajících podpisů.
- Kruhový podpis (ring signature) – používá se k prokazování příslušnosti ke skupině uživatelů. Může být použit jako podpis za skupinu, ale se zachováním anonymity podepisujícího a s možným nesouhlasem ostatních členů skupiny.
- Skupinový podpis (group signature) – slouží pro skrytí podepisující strany ve skupině oprávněných uživatelů. [6]

3 PRÁVNÍ ÚPRAVA ELEKTRONICKÉHO PODPISU V ČR

V České republice je z pohledu elektronického podpisu klíčovým legislativním dokumentem zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů. Tento zákon byl přijat v roce 2000 a byl později novelizován zákonem č. 226/2002 Sb., který upravil §19 odst.1, tedy že podání je možno učinit písemně, ústně do protokolu anebo v elektronické podobě podepsané zaručeným elektronickým podpisem.

Další novelizací zákona o elektronickém podpisu byl zákon č. 517/2002 Sb**.,** ve kterém se slova „Úřad pro ochranu osobních údajů“ nahrazují slovy „Ministerstvo informatiky“.

Zásadní novelou zákona o elektronickém podpisu se stal zákon č. 440/2004 Sb. Zákon doplněn o vysvětlení pojmů jako elektronické značky, časová razítka, systémové certifikáty, dále o podmínky certifikačních autorit. Mění také slovo „upravuje“ za slova „v souladu s právem Evropských společenství.

Posledním úplným zněním zákona č. 227/2000 Sb. je zákon č. 486/2004 Sb., který představuje úplné znění zákona o elektronickém podpisu, vyhlášeno předsedou vlády ve sbírce ze dne 9.9.2004. [7]

Klíčovou roli kontrolního a akreditačního orgánu v duchu zákona v současné době zastává Ministerstvo vnitra ČR. Mezi jeho hlavní povinnosti patří zejména dozor nad dodržování zákona o elektronickém podpisu, udělování akreditací poskytovatelům certifikačních služeb a vyhodnocování shody nástrojů elektronického podpisu s požadavky stanovenými zákonem. 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.

Zákon o elektronickém podpisu deklaruje, že vychází ze Směrnice Evropského parlamentu a Rady 1999/93/ES.

Tato směrnice se zabývá elektronickými podpisy používanými především pro účely autentizace (ověření identity subjektu) a aplikací zaručených elektronických podpisů, které mají být právně ekvivalentní klasickým, ručně psaným podpisům. Směrnice předpokládá použití

elektronického podpisu jako nástroje k ověřování pravosti dat elektronickou cestou v mnoha oblastech lidské činnosti.

Jedním z klíčových přínosů Směrnice je zavedení společné terminologie ve vztahu k elektronickému podpisu. Ta se potom přenáší i do lokálních legislativ a zvyšuje tak srozumitelnost pojmů. [8]

4 VÝKLAD POJMŮ SOUVISEJÍCÍCH S ELEKTRONICKÝM PODPISEM

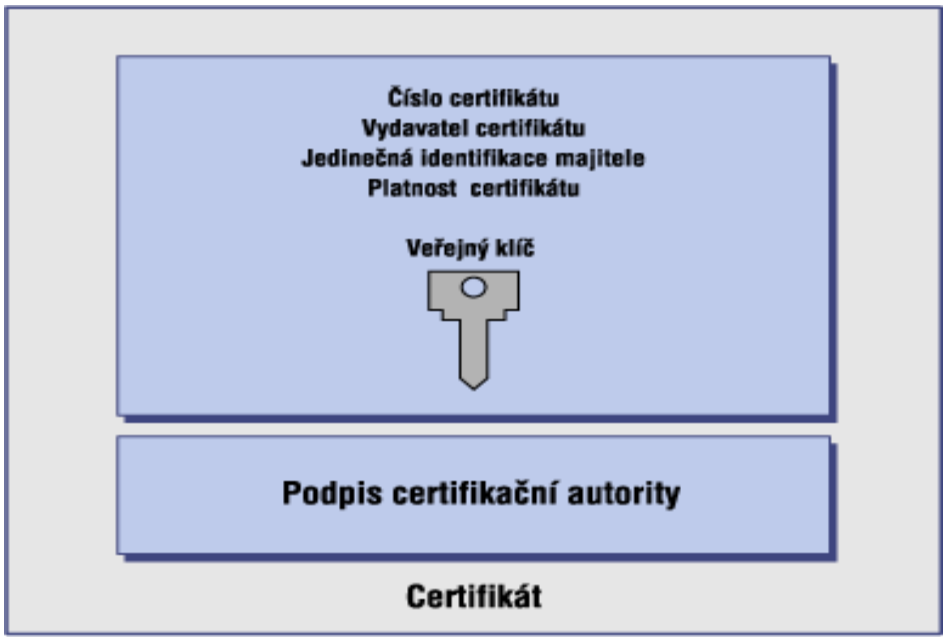
4.1 Certifikát

Certifikát slouží k důvěryhodnému předání dat pro ověřování elektronického podpisu podepisující osoby. Jedná se o datovou zprávu, která je vydána poskytovatelem certifikačních služeb a která spojuje data pro ověřování podpisu s podepisující osobou a umožňuje s dostatečnou spolehlivostí a věrohodností ověřit, ke které fyzické osobě se data pro ověřování elektronického podpisu vztahují. [9]

Vydáním certifikátu poskytovatel stvrzuje, že data pro ověřování elektronického podpisu patří určité osobě a že ve spojení s daty pro vytváření elektronického podpisu podepisující osoby vykonávají požadované funkce.

Certifikát tedy představuje spojení mezi daty pro ověřování elektronického podpisu a identitou určité osoby. Identitu podepisující osoby podle typu certifikátu může poskytovatel zjišťovat různými způsoby, v některých případech postačí e-mailová adresa, v jiných je nutné osobně prokázat totožnost příslušnými doklady.

Zákon o elektronickém podpisu neupravuje jiné předávání dat pro ověřování elektronického podpisu než prostřednictvím kvalifikovaných certifikátů. V praxi jsou používány i jiné způsoby nebo certifikáty, které nejsou kvalifikované ve smyslu zákona o elektronickém podpisu. Certifikáty jako standardní způsob předávání dat pro ověřování elektronického podpisu používá například Microsoft Outlook nebo Outlook Express. Data pro ověřování elektronického podpisu lze také vystavit v internetové síti veřejných klíčů či na jakémkoliv jiném vhodném místě, kde se s nimi mohou seznámit ti, se kterými má podepisující osoba v úmyslu komunikovat. [9]



Obr. 1. Certifikát (www.ica.cz)

4.2 Poskytovatel certifikačních služeb

Poskytovatel certifikačních služeb je autorita, která je důvěryhodná pro uživatele certifikačních služeb, to znamená, je důvěryhodná jak pro podepisující osoby, kterým vydává certifikáty, tak pro osoby, které se spoléhají na podpisy, s nimiž jsou tyto certifikáty spojeny. Certifikační autorita zejména vydává certifikáty a za stanovených podmínek je zneplatňuje. Vydané certifikáty podepisuje svým elektronickým podpisem, čímž je chrání proti případné modifikaci, a je identifikovatelná jako subjekt, který je vydal. [9]

Certifikační autorita může některé činnosti zajišťovat prostřednictvím jiných subjektů, například služby registračních autorit, vždy však na ní zůstává odpovědnost za poskytované služby.

4.3 Časové razítko

Časové razítko je údaj, který lze přidat k elektronicky podepsané datové zprávě a který stvrzuje, že datová zpráva existovala dříve, než k ní bylo toto razítko přidáno. Takové stvr-

zení musí učinit někdo důvěryhodný a nezávislý na podepisující osobě a příjemci zprávy. Může se tak jednat o jednu ze služeb, které poskytuje poskytovatel, nebo ji může nabízet jiný subjekt.

U datových zpráv, u kterých se předpokládá dlouhodobé uchování, je možné například díky použití časového razítka prokázat, že datová zpráva byla odeslána v době platnosti příslušného certifikátu.

Vzhledem k tomu, že jiný způsob prokázání času, kdy byla datová zpráva elektronicky podepsána, je velmi problematický, je možné předpokládat rozvoj služeb časových razítek.

[9]

Zákon o elektronickém podpisu používání časových razítek neupravuje.

4.4 Data pro vytváření a data pro ověřování elektronického podpisu

Data pro vytváření elektronického podpisu slouží, jak název napovídá, pro jeho vytvoření. Nestačí však zprávu elektronicky podepsat, je nutné ještě zajistit, aby mohlo být ověřeno, kdo právu podepsal. K tomu slouží data pro ověřování elektronického podpisu, která musí být odpovídající datům pro vytváření, tj. obojí data musí být taková, aby ve spojení zajišťovala požadované funkce. Data pro ověřování elektronického podpisu se nazývají „veřejný klíč“ a data pro vytváření elektronického podpisu „soukromý klíč“. Data pro vytváření podpisu musí podepisující osoba uchovat v tajnosti, data pro ověřování podpisu jsou naopak určena ke zveřejnění. Data pro ověřování podpisu je nutné bezpečně předávat mezi podepisující osobou a příjemcem elektronicky podepsané zprávy. K tomuto bezpečnému předání může sloužit certifikát, což je datová zpráva, která spojuje data pro ověřování podpisu s osobou, které byl vydán a umožňuje ověřit její totožnost.

Data pro vytváření elektronického podpisu mohou být uložena na pevném disku počítače, na disketě, na čipové kartě nebo přenosném bezpečnostním modulu. Je vhodné, aby přístup k těmto datům byl chráněn přístupovým heslem, frází, PIN kódem apod., které zná jen jejich vlastník. Volba nosiče by měla odpovídat účelu, pro který bude elektronický podpis používán. [9]

4.5 Podepisující osoba

Podepisující osobou ve smyslu zákona o elektronickém podpisu může být pouze fyzická osoba. [1]

Stejně jako v případě vlastnoručního podpisu není přípustné, aby se elektronicky podepisovala právnická osoba, byť v případě elektronického podpisu by z technického hlediska teoreticky taková možnost byla, není to povoleno. Stejně jako jsou v organizaci (firmě apod.) určeni pracovníci, kteří jsou oprávněni svým podpisem opatřovat listinné dokumenty a jednat tak jménem právnické osoby, je potřeba analogicky postupovat i při elektronickém podepisování. V certifikátu v položce „účel“ lze konstatovat oprávnění fyzické osoby k podepisování jménem osoby právnické. Fyzická osoba se tak může elektronicky podepisovat jménem právnické osoby a osoba spoléhající se na podpis v certifikátu vidí, že tato osoba je k tomu oprávněna. [9]

Bezpečnost elektronického podepisování je do značné míry závislá na chování podepisující osoby, zejména na její schopnosti uchovat v tajnosti svá data pro vytváření elektronického podpisu (soukromý klíč). Pokud hrozí nebezpečí zneužití jejich dat pro vytváření elektronického podpisu, je podepisující osoba v této skutečnosti povinna uvědomit poskytovatele, který jí kvalifikovaný certifikát vydal. Další povinností podepisující osoby je podávat přesné, pravdivé a úplné informace poskytovateli certifikačních služeb. [9]

Fyzická osoba může mít libovolný počet certifikátů. Jiné certifikáty mohou akceptovat banky, jiné instituce veřejné správy. S „univerzálními“ certifikáty, které by akceptovali všichni potencionální příjemci elektronicky podepsaných zpráv, se v současné době ani v ČR ani v zahraničí nepočítá. Je to obdobná situace, jako když osoba využívá služeb více bank a od každé má jednu platební kartu. [9]

4.6 Datová zpráva

S tímto pojmem se lze v souvislosti s elektronickým podpisem setkat především ve dvou významech – datovou zprávou je to, co je podepisováno a současně je datovou zprávou i certifikát.

Elektronicky je možné podepsat jakoukoliv datovou zprávu, tedy vše, co existuje v elektronické podobě. Může to být e-mailová zpráva, obrázek, program, databázový soubor, makro atd. [9]

4.7 Šifrování

Cílem šifrování zpráv je zabránit odposlouchávání či zneužívání zpráv na jejich cestě od odesílatele k příjemci.

Známe dvě metody šifrování, a to šifrování symetrické a asymetrické.

To jednodušší, šifrování symetrické, funguje na základě jednoho klíče, který je znám oběma komunikujícím osobám – odesílateli zprávy a jejímu příjemci. Zpráva se před odesláním zašifruje pomocí klíče odesílatele a příjemce si tuto zprávu dešifruje stejným klíčem, který mu musí být předán.

Naproti tomu šifrování asymetrické funguje na základě užití dvou klíčů – klíče soukromého a veřejného. Zpráva je odesílatelem zašifrována jedním klíčem a příjemcem dešifrována klíčem druhým. [10]

4.8 Veřejný klíč

Jedná se o veřejnou část páru klíčů uživatele, která je určena pro ověřování elektronického podpisu a pro šifrování. [9]

4.9 Soukromý klíč

Jedná se o tajnou část páru klíčů uživatele, která je určena pro vytváření elektronického podpisu. Vzhledem k jejímu použití je třeba pro tuto část zajistit co nejvyšší bezpečnost. Z tohoto důvodu se v současnosti pro její uchování využívá různých hardwarových prostředků, jako jsou čipová karta či USB. [9]

4.10 Elektronická značka

Elektronickou značkou podle Zákona o elektronickém podpisu rozumíme 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 certifikátu,
- byly vytvořený a připojeny k datové zprávě pomocí prostředku pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou,
- jsou k datové zprávě, ke které se vztahují připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat. [1]

4.11 e-Government

Pod pojmem e-Government si lze představit elektronizaci státní správy a samosprávy.

Mezi stěžejní výhody této elektronizace patří:

- rychlost a kvalita služeb občanům,
- jednoduchost, uživatelská přívětivost,
- úřední hodiny pro podání 24 hodin denně, 7 dní v týdnu,
- finanční úspory,
- transparentnost procesů a rozhodování.

Bez elektronické komunikace si e-Government nelze představit. Není efektivní mít možnost vyplnit si formulář elektronicky, poté si ho vytisknout a přinést na úřad, vystát si frontu a následně předat papírový formulář úředníkovi, který ho přepíše do počítače.

Daleko výhodnější je předat elektronický dokument elektronickou cestou. [8]

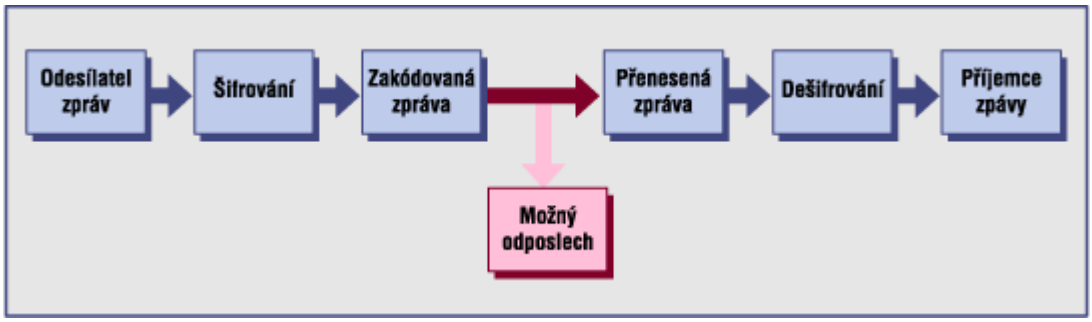
5 ŠIFROVACÍ METODY

Výměna informací v elektronické podobě je trendem dnešní doby. Ne každá informace je však určena každému. Jinými slovy, data je třeba dostatečně chránit.

Nabízí se tedy možnost logické ochrany dat, neboli šifrování. Znamená to zašifrovat data na straně odesílatele, odeslat je a na straně příjemce zase dešifrovat.

Kvalita logické ochrany je dána šifrovací metodou, typem užitého algoritmu, jeho aplikací a délkou šifrovacího klíče. [9]

Přenos zpráv šifrovaných kanálem je znázorněn v následujícím obrázku (Obr. 2.).



Obr. 2. Přenos zpráv šifrovaným kanálem (www.ica.cz)

V zásadě rozlišujeme dvě šifrovací metody, a to, symetrickou kryptografii a asymetrickou kryptografii.

Naproti tomu existuje odvětví, které se nazývá kryptoanalýza. Jde o vědu o analýze a probíjení zakódovaných informací. Ke kryptoanalýze je třeba mnoho analytického myšlení, aplikace matematických metod, hledání cest, trpělivost a štěstí.

5.1 Symetrická kryptografie

Jedná se o metodu symetrické šifry. Znamená to, že stejný klíč, který byl užit k zašifrování zprávy na straně odesílatele, bude užit i na straně příjemce pro dešifrování zprávy. Z toho

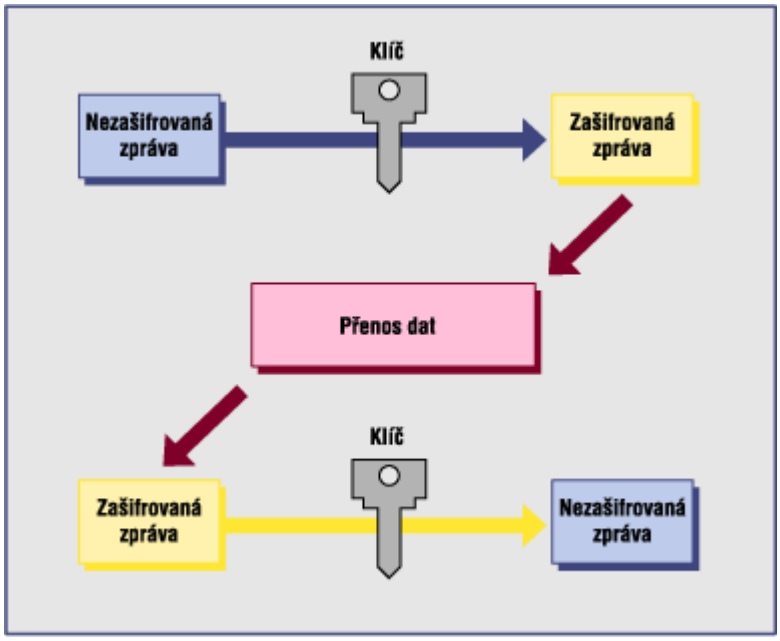
vyplývá nutnost před začátkem komunikace předat důvěryhodným kanálem šifrovací klíč spolu s dalšími údaji, konkrétním typem algoritmu, druhé straně. [9]

Symetrických šifrovacích algoritmů je celá řada – IDEA, AES, DES, 3DES, CAST a mnoho dalších.

Současná komerčně dostupná výpočetní technika aplikuje tyto algoritmy (např. DES, TRIPLEDES, IDEA, AES) téměř v reálném čase.

Použití symetrických algoritmů představuje způsob, jak zabezpečit důvěrnost transakcí definovaným způsobem s možností přesného stanovení hrozeb, kterým toto zabezpečení odolává. Problémem těchto algoritmů je, že nelze určit, která strana zprávu odeslala a která přijala. [10]

V následujícím obrázku (Obr. 3.) můžete vidět schéma symetrického šifrování.

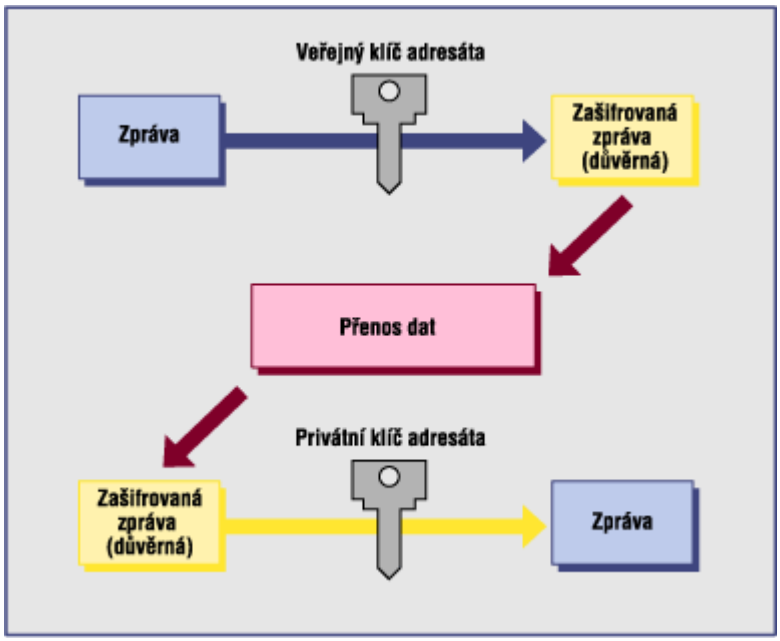


Obr. 3. Symetrické šifrování (www.ica.cz)

5.2 Asymetrická kryptografie

Na rozdíl od symetrické kryptografie, u které je využíváno jednoho klíče, se zde užívá dvojice klíčů. Tuto dvojici klíčů si vygeneruje uživatel pomocí některého z běžně dostupných softwarových produktů a stává se tak jejich jediným majitelem.

Princip asymetrické kryptografie spočívá v tom, že data šifrovaná jedním z klíčů lze v rozumném čase dešifrovat pouze se znalostí druhého z dvojice klíčů a naopak, schéma postupu asymetrického šifrování je zobrazeno v obrázku, který následuje (Obr. 4.)



Obr. 4. Asymetrické šifrování (www.ica.cz)

První z klíčů, klíč privátní je s maximální bezpečností ukrýván majitelem a klíč druhý je zveřejněn. Znamená to, že známe-li vlastníka veřejného klíče, pomocí kterého jsme zprávu dešifrovali, známe odesilatele.

Základní vlastností šifrování na bázi asymetrických algoritmů je skutečnost, že je relativně jednoduché za využití veřejného klíče a veřejným klíčem šifrované zprávy je velice obtížné získat původní zprávu. [9]

Mezi nejznámější asymetrické šifrovací algoritmy patří například RSA, DSA, DH. [10]

5.3 Hybridní kryptografie

Hybridní kryptografie je kombinací kryptografie symetrické a asymetrické. Spojuje výhody symetrické kryptografie – rychlost šifrování a dešifrování s výhodami asymetrické kryptografie – menší počet klíčů, nižší nároky na jejich správu.

PGP (Pretty Good Privacy) – systém, který byl vyvinut pro autentizaci a šifrování e-mailové komunikace, je typickým příkladem kombinovaného šifrovacího systému. Navenek se jeví jako program s veřejným šifrovacím klíčem, plně využívající asymetrického šifrování. To se však ve skutečnosti používá pouze pro zakódování klíče symetrické šifry, kterou je pak zašifrována samotná zpráva. Digitálním podpisem je kontrolní součet - otisk zprávy (hash), který je zašifrován asymetrickou šifrou. [11]

5.4 Hash funkce

Díky tomu, že asymetrické šifrování je výpočetně náročné a šifrování delších zpráv by trvalo dlouho, navíc připojením celé šifrované zprávy bychom zvětšovali datový objem původní zprávy, nešifruje se celá zpráva, ale pouze její tzv. otisk (hash).

Hash neboli otisk je jednocestná funkce, která nám z libovolně dlouhého textu vytvoří krátký řetězec konstantní délky. Takto vzniklý řetězec (hash, otisk) má za úkol maximálně charakterizovat původní text. Jednocestnou funkcí se rozumí algoritmy, které nejsou výpočetně náročné. Je však výpočetně velice náročné k výsledku nalézt původní text.

Kvalitní jednocestné funkce pro výpočet otisku by měly dát výrazně jiný výsledek při drobné změně původního textu. Počítáme-li například otisk pro digitální podpis z textu nesoucí platební příkaz, pak by bylo nemilé, kdy se nám po připsání nuly k převáděné částce otisk nezměnil. [10]

Mezi hashovací funkce patří například: MD2, MD4, MD5, SHA-1, SHA-2(256,384,512), LM, NT, VNC Hash a mnoho dalších. [10]

5.5 Ochrana dat

Tak jako je důležité chránit dokumenty v papírové podobě, je nutné zabezpečit i ty elektronické.

5.5.1 Fyzická ochrana dat

Jedná se především o ochranu nosičů dat (CD, DVD, HDD) před neoprávněnými osobami či přírodními jevy jako je například vlhko, sluneční záření a podobně. [12]

5.5.2 Logická ochrana dat

Mezi jeden z nejdůležitějších prostředků ochrany dat patří již zmiňované šifrování, tedy kryptografie. Jejím úkolem je zajistit důvěryhodnost těchto dat a zamezit nepovolaným osobám v přístupu k těmto datům. [12]

6 ELEKTRONICKÁ PODATELNA

Elektronická podatelna je definována ve vyhlášce č. 496/2004 Sb**.** o elektronických podatelnách, která stanoví postupy orgánů veřejné moci uplatňované při přijímání a odesílání datových zpráv prostřednictvím elektronické podatelny a strukturu údajů kvalifikovaného certifikátu, na základě kterých je možné podepisující osobu při přijímání datových zpráv prostřednictvím elektronické podatelny jednoznačně identifikovat. [13]

Dále se k elektronickým podatelnám vztahuje nařízení vlády č. 495/2004 Sb., které definuje organizačně technická opatření pro orgány veřejné moci k zajištění postupů uplatňovaných při přijímání a odesílání datových zpráv prostřednictvím elektronické podatelny.

[14]

Povinnost zřídit jedno či více takových pracoviště je uložena tímto nařízením orgánům veřejné moci, pokud pro ně ze zvláštních předpisů vyplývá povinnost přijmout podání učiněné v elektronické podobě, podepsané elektronicky, anebo stanoví-li zvláštní právní předpis právo těchto orgánů činit úkony v elektronické podobě. Tato povinnost se vztahuje rovněž na územní samosprávné celky provádějící výkon státní správy v rámci přenesené působnosti.

Povinnosti uložené tímto nařízením orgánům veřejné moci

Vydané nařízení vlády ukládá orgánům veřejné moci:

1. zřídit podle povahy a rozsahu své činnosti jedno nebo více pracovišť pro příjem a odesílání datových zpráv vybavených potřebnými zařízeními připojenými k veřejné datové síti, splňující požadavky na technické a programové vybavení podle standardů a umožňující používání zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb,
2. pověřit zaměstnance vytvářením a ověřováním zaručených elektronických podpisů,

3. organizovat práce v elektronické podatelně tak, aby bylo zajištěno přijímání a odesílání datových zpráv a neprodlená kontrola přijatých podání,
4. zajistit příjem podání v elektronické podatelně i v případě, že je přímo předáno na technickém nosiči dat,
5. zveřejnit elektronické adresy svých elektronických podatelen a seznam kvalifikovaných certifikátů příslušných zaměstnanců nebo elektronické adresy, na nichž se kvalifikované certifikáty nacházejí.

Elektronické podatelny musí být vybaveny potřebnými zařízeními připojenými k veřejné datové síti, popřípadě jiným sítím. Zařízení musí umožňovat používání zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb.

Elektronická podatelna není pouze e-mailová adresa, zveřejněná úřadem, její funkce je podstatně významnější, neboť je vstupním bodem pro elektronický oběh a zpracování dokumentů v organizaci. [3]

7 MARKETINGOVÝ VÝZKUM

Marketingový výzkum je souhrn aktivit, které se uskutečňují na podporu marketingového rozhodování.

Marketingový výzkum je cílevědomá a organizovaná činnost, která spočívá ve shromažďování, specifikaci, analýze a interpretaci informací, které umožňují:

- porozumět prostředí,
- identifikovat příležitosti, které se mohou naskytnout,
- formulovat směry marketingové činnosti,
- hodnotit její výsledky. [15]

7.1 Etapy marketingového výzkumu

7.1.1 Identifikace problému

Jedná se o převedení daného problému do podoby, ve které může být řešitelný. Základem tedy je problém přesně definovat, stanovit jeho specifické rysy a pokusit se o předběžnou formulaci hypotézy.

7.1.2 Orientační analýza situace

Jde o ověření si hypotézy na základě shromáždění dostupných informací a názorů na problematiku. Hledá se oblast možného řešení problému. Problém je třeba analyzovat.

7.1.3 Vytvoření plánu výzkumného projektu

Poté, co byl problém definován, byl nalezen směr jeho řešení, je nutno vytvořit určitý plán samotného výzkumu.

Tento plán výzkumu obsahuje:

a) specifikaci informací, které budou shromažďovány,
b) způsob sběru informací s uvedením formy,
c) metody zpracování dat – jaká metoda bude použita,
d) rozpočet výzkumu,

e) stanovení přesných specifických úkolů,
f) kontrola plánu – tzv. pretest, díky němuž je možno opravit případné chyby v postupech.

7.1.4 Sběr dat

Tento sběr dat se sestává ze samotného shromažďování dat. Týká se jak informací primárních, tak i sekundárních, tedy studia dokumentů.

7.1.5 Zpracování shromážděných dat

Jde o data především primární, které je nutno:

a) upravit – pověřit jejich přesnost a úplnost,
b) klasifikovat – získané údaje rozdělit do kategorií a tříd,
c) kódovat – převést slovní výrazy do numerických znaků,
d) technicky zpracovat – vyjádřit výsledky výzkumu pomocí potřebných tabulek a grafů.

7.1.6 Interpretace výsledků

Závěry představují stručné a jasné slovní konstatování s doporučením, konečným cílem výzkumu. [15]

7.2 Dotazování

Pro svou práci jsem si vybrala jednu z typických metod marketingového výzkumu - dotazování. Tato metoda umožňuje zobrazení rozdílů v mínění respondentů.

Dotazování znamená kontakt s respondentem prostřednictvím záznamového média (písemně – pomocí dotazníků). Díky dotazování máme získat informace v určitých vybraných charakteristikách zkoumaných jevů, s cílem získat co nejvěrohodnější údaje. Jedná se o typickou metodu marketingového výzkumu, která umožňuje zobrazení rozdílů v mínění respondentů. [15]

Mezi základní fáze dotazování patří:

7.2.1 Adaptace (úvod)

- vysvětlení cíle,
- popsání způsobu vyplňování otázek,
- snaha motivovat respondenta, vzbudit jeho zájem.

7.2.2 Kontakt

- cílem je postupně uvést respondenty do problému,
- dotazování musí být snadné, bezproblémové, s jednoduchými a jasnými odpověď-mi.

7.2.3 Dosažení vytyčeného cíle

- sběr základních informací pro řešení stanoveného úkolu,
- kontrola relevantnosti odpovědí,
- snaha o udržení zájmu respondentů.

7.2.4 Závěr dotazování

- otázky odstraňující napětí,
- umožnění emocionálního vyjádření, případně vlastního názoru. [15]

7.3 Typy otázek využívaných při dotazování

7.3.1 Funkcionální otázky

- kontaktní,
- funkcionálně psychologické – slouží k odstranění napětí při přechodu od jednoho tématu k druhému a také k odstranění stereotypů,

- filtrační – otázky, kterými zjistíme, zda respondent patří ke skupině, jíž se otázka týká,
- kontrolní – jedná se o otázky, kterými řešíme problém, a to, zda získáváme věrohodná data.

7.3.2 Obsahové otázky

- otázky o faktech – jde například o zjištění věku, pohlaví, apod.,
- otázky o vědomostech a znalostech,
- otázky o mínění, postojích a motivech chování.

7.3.3 Otevřené otázky

- odpověď na tyto otázky vytváří sám dotazovaný,
- jde o sdělení vlastního názoru,
- tyto otázky jsou obtížně zpracovatelné avšak mají vysokou vypovídací schopnost.

7.3.4 Uzavřené otázky

Uzavřené otázky nabízí respondentovi jednu nebo několik možných odpovědí. Tyto otázky jsou náročné na navrhnutí jednotlivých možných odpovědí:

- dichotomické otázky – nabízí dvě možné volby (ano x ne),
- trichotomické otázky – nabízí tři možné volby (ano x ne x nevím),
- polytomické otázky – nabízí více možností,
  - výběrové otázky – vybírá se jen jedna odpověď,
  - výčtové otázky – umožňují vybrat jednu nebo více odpovědí,
- baterie otázek – zde jsou soustředěny odpovědi na řadu otázek, na které bychom se jinak ptali odděleně,
- škálové otázky.

7.3.5 Polootevřené otázky

Polootevřené otázky představují kombinaci otevřených a uzavřených otázek. Respondent má na výběr několik možných odpovědí. V případě, že si respondent žádnou z nabízených odpovědí nevybere, má možnost sdělit svůj názor. [15]

II. PRAKTICKÁ ČÁST

8 MARKETINGOVÝ VÝZKUM U INSTITUCÍ VEŘEJNÉ SPRÁVY OLOMOUCKÉHO KRAJE A JEHO VYHODNOCENÍ

Tato praktická část je věnována analýze marketingového výzkumu, jehož cílem bylo zmapovat postoje a názory zaměstnanců veřejné správy Olomouckého kraje k možnostem využívání elektronického podpisu u elektronických podatelen a zjistit další skutečnosti týkající se tohoto tématu.

Průzkum byl prováděn v prvním čtvrtletí 2008 ve vybraných institucích veřejné správy Olomouckého kraje (Krajský úřad Olomouc, Městský úřad Uničov, Městský úřad Šternberk, Městský úřad Litovel, Městský úřad Jeseník, Finanční úřad Šternberk, Finanční úřad Šumperk a Okresní správa sociálního zabezpečení Olomouc) formou dotazníkového šetření.

Otázka č.1: Využíváte elektronický podpis při své práci?

Tab. 1. Vyhodnocení otázky č. 1

	Absolutní četnost	**Relativní četnost**
ANO	24	27%
NE	**64**	**73%**
celkem	88	100%

Jedná se o informativní otázku, ne příliš náročnou na respondenty. Z celkového počtu osmdesáti osmi dotázaných odpovědělo dvacet čtyři respondentů, že využívá elektronický podpis při své každodenní práci a zbývajících šedesát čtyři účastníků dotazování elektronický podpis při své práci nevyužívá.

U respondentů, kteří odpověděli na první otázku kladně, tedy že elektronický podpis využívají, otázka pokračovala. Zajímalo mě, jak často jej využívají.

Tab. 2. Vyhodnocení podotázky k otázce č. 1

	Absolutní četnost	**Relativní četnost**
spíše ne	2	8%
občas využívám	5	21%
často využívám	**9**	**38%**
využívám každodenně	8	33%
celkem	24	100%

Elektronický podpis každodenně či často využívá, jak ukazuje výše uvedená tabulka (Tab. 2.), sedmnáct (71%) z celkových dvaceti čtyř uživatelů elektronických podatelen.

Otázka č.2: Víte co to elektronická podatelna je?

Tab. 3. Vyhodnocení otázky č.2

	Absolutní četnost	**Relativní četnost**
ANO	**83**	**94%**
NE	5	6%
celkem	88	100%

Průzkum ukázal, že většina dotazovaných, osmdesát tři z osmdesáti osmi účastníků průzkumu (94%) ví, co to elektronická podatelna je. Vypovídá to o velké informovanosti zaměstnanců institucí veřejné správy.

Otázka č.3: Má Váš úřad (Vaše organizace) zřízenou elektronickou podatelnu?

Tab. 4. Vyhodnocení otázky č.3

	Absolutní četnost	**Relativní četnost**
ANO	**82**	**93%**
NE	6	7%
celkem	88	100%

Když jsem tuto otázku zařazovala do dotazníku, dlouho jsem přemýšlela, jestli není bezpředmětná a nic vypovídající. Očekávala jsem stoprocentní úspěšnost odpovědi ANO, tedy, že dotazovaní (zaměstnanci veřejné správy), vědí, jestli má jejich úřad či jiná instituce veřejné správy, kde jsou zaměstnaní, zřízenou elektronickou podatelnu.

Výsledky však ukázaly, že pět respondentů, což představuje 7% všech dotázaných, to nevědělo.

Pokud ANO, využívají ji spíše občané nebo firmy?

Tab. 5. Vyhodnocení podotázky k otázce č.3

	Absolutní četnost	**Relativní četnost**
spíše občané	6	7%
spíše firmy	9	11%
občané i firmy	24	29%
nedokáži posoudit	**43**	**52%**
celkem	82	100%

Tato podotázka byla spíše o úsudku a soukromém tipu dotázaných než o jejich znalosti. Neboť je nemožné, aby přesně každý zaměstnanec věděl, jestli elektronickou podatelnu využívají více občané či firmy. Zajímal mě samotný názor respondentů. Četnost využití

elektronické podatelny fyzickými nebo právnickými osobami je spíše otázkou na statistiky či někoho kompetentního, který si dělá záznamy o využívání elektronické podatelny.

Přesně podle mého předpokladu více než polovina oslovených na tuto otázku odpověděla, že nedokáží posoudit, kým je více elektronická podatelna využívána, 29% respondentů pak uvedlo, že ji využívaní občané i firmy.

Otázka č.4: Absolvovali jste specializovaná školení v oblasti elektronického podpisu nebo elektronické podatelny?

Tab. 6. Vyhodnocení otázky č.4

	Absolutní četnost	**Relativní četnost**
ANO	27	31%
NE	**61**	**69%**
celkem	88	100%

Je překvapující, jak malé procento respondentů se účastnilo specializovaných školení v oblasti elektronického podpisu či elektronické podatelny. Jedná se přibližně o jednu třetinu všech oslovených.

Pokud ANO, jaké oblasti se týkalo?

Tab. 7. Vyhodnocení podotázky k otázce č.4 – odpověď ANO

	Absolutní četnost	**Relativní četnost**
pouze el.podpis	1	4%
pouze el.podatelna	4	15%
obojí	**22**	**81%**
celkem	27	100%

81 % respondentů, kteří odpověděli na otázku číslo 7 kladně, tedy že absolvovali školení týkající se elektronického podpisu či elektronické podatelny, absolvovali školení týkající se obou těchto oblastí. Školení pouze o elektronické podatelně absolvovalo 15% oslovených a jen 4% dotázaných uvedlo, že absolvovalo odborné školení týkající se pouze elektronického podpisu.

Pokud NE, měli byste zájem o absolvování těchto školení?

Tab. 8. Vyhodnocení podotázky k otázce č.4 – odpověď NE

	Absolutní četnost	**Relativní četnost**
zájem nemám	15	25%
zájem o el.podpis	11	18%
zájem o el.podatelnu	0	0%
zájem o obojí	**22**	**36%**
v budoucnu uvažuji	13	21%
celkem	61	100%

Žádný z oslovených neměl zájem účasti na školení týkajícího se pouze elektronické podatelny. Velký zájem byl o komplexní školení, tedy o školení zaměřené na elektronický podpis i elektronickou podatelnu. 21 % oslovených pak uvažuje do budoucna, že by se těchto školení chtělo zúčastnit, neboť to budou potřebovat ke své práci.

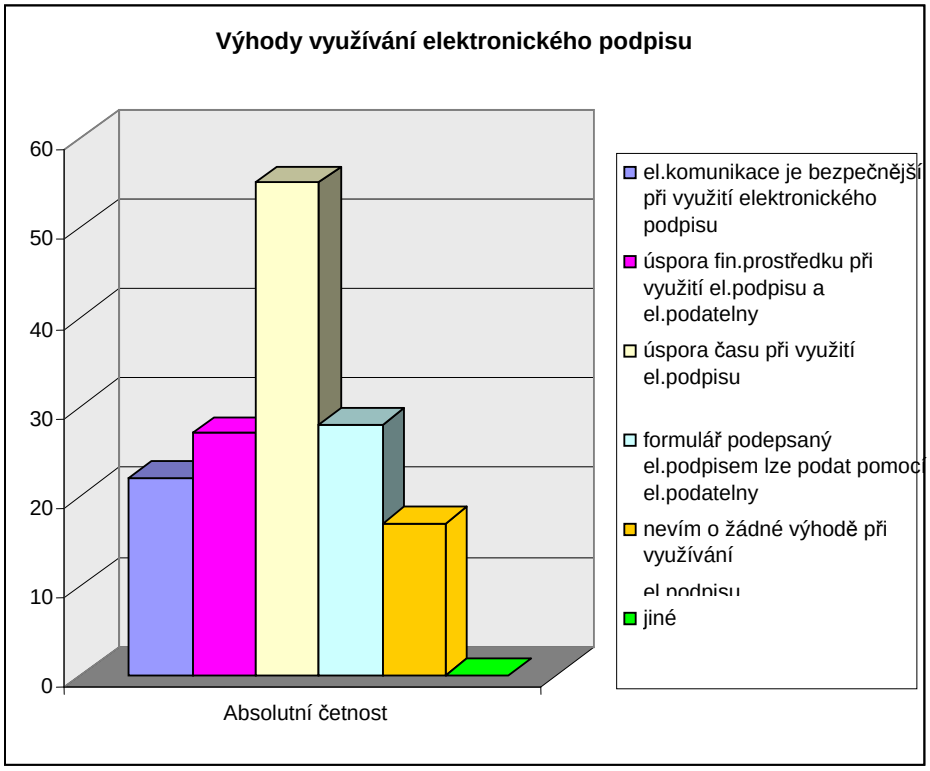
Otázka č.5: V čem spatřujete výhody využívání elektronického podpisu?

Tab. 9. Vyhodnocení otázky č.5

	Absolutní četnost	**Relativní četnost**
el.komunikace je bezpečnější při využití elektronického podpisu	22	15%
úspora finančních prostředků při využití el.podpisu a el.podatelny	27	18%
úspora času při využití el.podpisu	**55**	**37%**
formulář podepsaný el.podpisem lze podat pomocí el.podatelny	28	19%
nevím o žádné výhodě při využívání el.podpisu	17	11%
jiné	0	0%
celkem	149	100%

V důsledku možnosti volby více odpovědí na tuto otázku jsou odpovědi následující: 37% dotázaných spatřuje jako největší výhodu úsporu času při využití elektronického podpisu, pro 19 % respondentů je největší výhodou poslat formulář podepsaný elektronickým podpisem pomocí elektronické podatelny, 18% oslovených považuje jako největší výhodu úsporu finančních prostředků, 15% účastníků průzkumu si myslí, že je elektronická komunikace bezpečnější při využití elektronického podpisu a 11% dotázaných neví o žádné výhodě spojené s využíváním elektronického podpisu.

Jednalo se o otázku polootevřenou s možností vyjádření vlastní myšlenky, názoru. Žádný z respondentů nenašel jinou výhodu než mnou nabídnutou.



Obr. 5. Výhody využívání elektronického podpisu

Otázka č.6: V čem naopak spatřujete nevýhody využívání elektronického podpisu?

Tab. 10. Vyhodnocení otázky č. 6

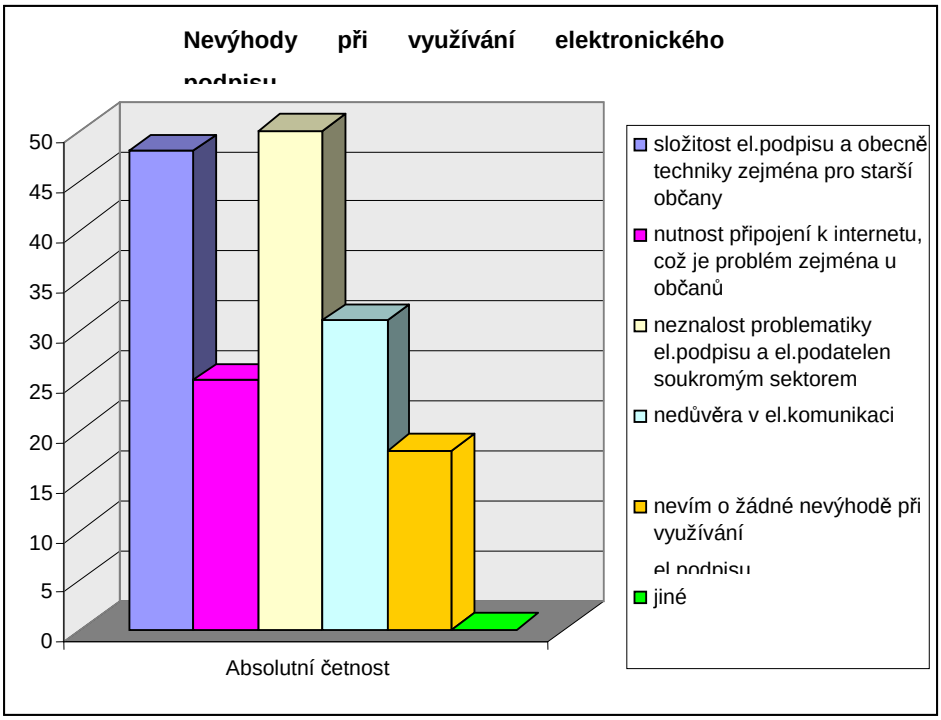
	Absolutní četnost	Relativní četnost
složitost el.podpisu a obecně techniky zejména pro starší občany	48	28%
nutnost připojení k internetu, což je problém zejména u občanů	25	15%
neznalost problematiky el.podpisu a el.podatelen soukromým sektorem	**50**	**29%**
nedůvěra v el.komunikaci	31	18%
nevím o žádné nevýhodě při využívání el.podpisu	18	10%
jiné	0	0%
celkem	172	100%

Stejně tak jako u předchozí otázky se jedná o otázku polootevřenou s možností vyjádření vlastního názoru dotázaných. Bohužel ani zde respondenti nenavrhli jinou nevýhodu využívání elektronického podpisu než tu, která se jim nabízela.

Za největší nevýhody využívání elektronického podpisu dotázaní považují neznalost problematiky elektronického podpisu a elektronických podatelen soukromým sektorem a složitost elektronického podpisu a obecně techniky zejména pro starší občany.

Obecně platí, že čím je člověk starší, tím méně se chce učit novým věcem. Samozřejmě jsou tak jak všude i zde výjimky, a najdou se starší občané, kteří rozumí technice daleko víc než ti mladší.

15% dotázaných uvedlo, že nevýhodou využívání elektronického podpisu je nutnost připojení k internetu. Myslím si, že kdybych udělala tento průzkum za pár let, bylo by procento rozhodně nižší, protože internet se rychle dostává do domácností, firem a škol.



Obr. 6. Nevýhody využívání elektronického podpisu

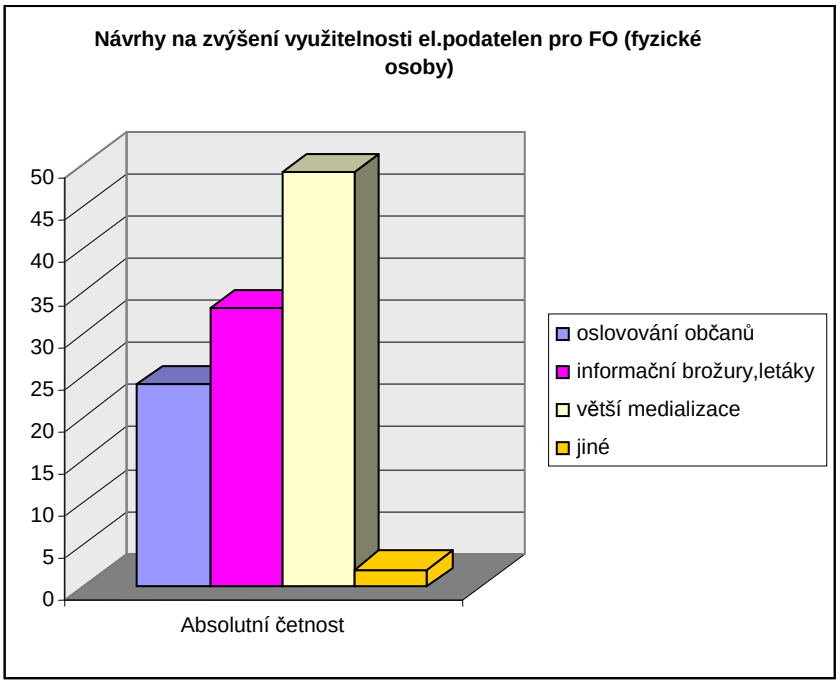
Otázka č.7: Jaké cesty byste navrhovali pro zvýšení využitelnosti elektronických podatelen pro FO (fyzické osoby)?

Tab. 11. Vyhodnocení otázky č. 7

	Absolutní četnost	Relativní četnost
oslovování občanů	24	22%
informační brožury,letáky	33	31%
větší medializace	**49**	**45%**
jiné	2	2%
celkem	108	100%

Jedná se o jednu z klíčových otázek dotazníku. Zajímalo mě, co by respondenti navrhovali pro zvýšení využitelnosti elektronických podatelen fyzickými osobami. Navrhla jsem možnosti jako oslovování občanů, informační brožury a letáky a větší medializaci tohoto problému. Nechala jsem i prostor pro vyjádření vlastního názoru. Ten vyjádřili pouze dva z respondentů, z nichž jeden navrhl reklamní spoty v televizi, což můžeme začlenit do již mnou nabídnuté možnosti – větší medializace, druhý dotázaný navrhl školení ze stran úřadů pro zájemce o tyto služby.

45% oslovených si myslí, že větší medializace může napomoci ke zvýšení využitelnosti elektronických podatelen fyzickými osobami, 31% dotázaných zvolilo jako prostředek zvýšení využitelnosti informační brožury a letáky a 22% oslovených zaměstnanců institucí veřejné správy Olomouckého kraje navrhlo oslovování občanů, kteří přijdou osobně na elektronickou podatelnu.



Obr. 7. Návrhy na zvýšení využitelnosti el.podatelen pro FO

Otázka č.8: Jaké cesty byste navrhovali pro zvýšení využitelnosti elektronických podatelen pro PO (právnické osoby)?

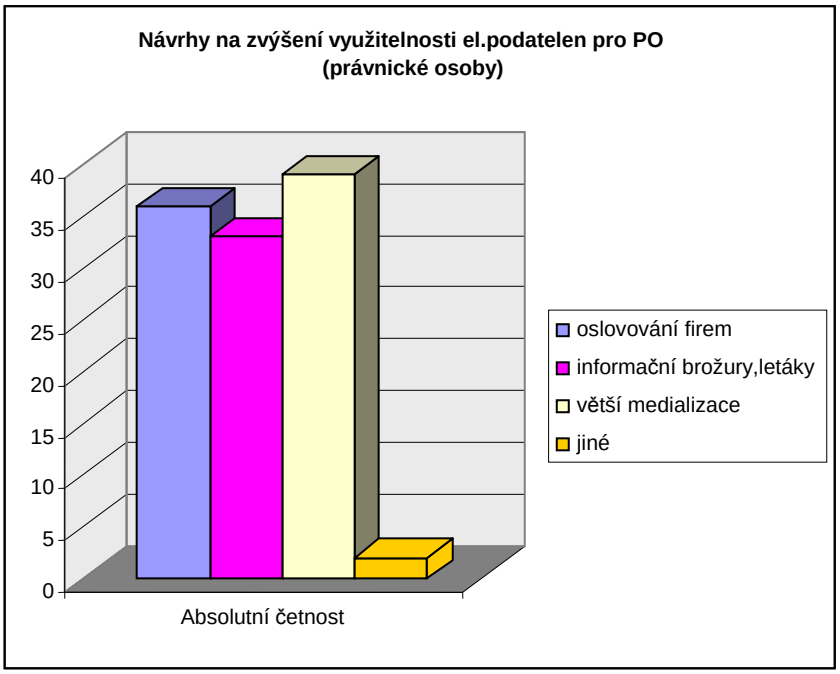
Tab. 12. Vyhodnocení otázky č. 8

	Absolutní četnost	**Relativní četnost**
oslovování firem	36	33%
informační brožury,letáky	33	30%
větší medializace	**39**	**35%**
jiné	2	2%
celkem	110	100%

Obdobně jako u předchozí otázky, kde mě zajímalo, co by respondenti navrhovali pro zvýšení využitelnosti elektronických podatelen fyzickými osobami, u této otázky jsem se zaměřila na právnické osoby. Mnou navržené možnosti byly taktéž shodné s otázkou předchozí, a to: oslovování firem, informační brožury a letáky a větší medializace. Respondenti měli také možnost vyjádřit vlastní názor. Návrhy na zvýšení využitelnosti elektronických

podatelen u právnických osob byly shodné s návrhy na zvýšení využitelnosti elektronických podatelen u fyzických osob. Navrhnuty byly reklamní spoty a školení ze stran úřadů pro zájemce o tyto služby.

35% oslovených poukazuje důraz na větší medializaci tohoto problému, 33% dotázaných si myslí, že právě oslovování firem má napomoci ke zvýšení využitelnosti elektronických podatelen a 30% respondentů zvolilo jako prostředek pro zvýšení využitelnosti informační brožury a letáky.

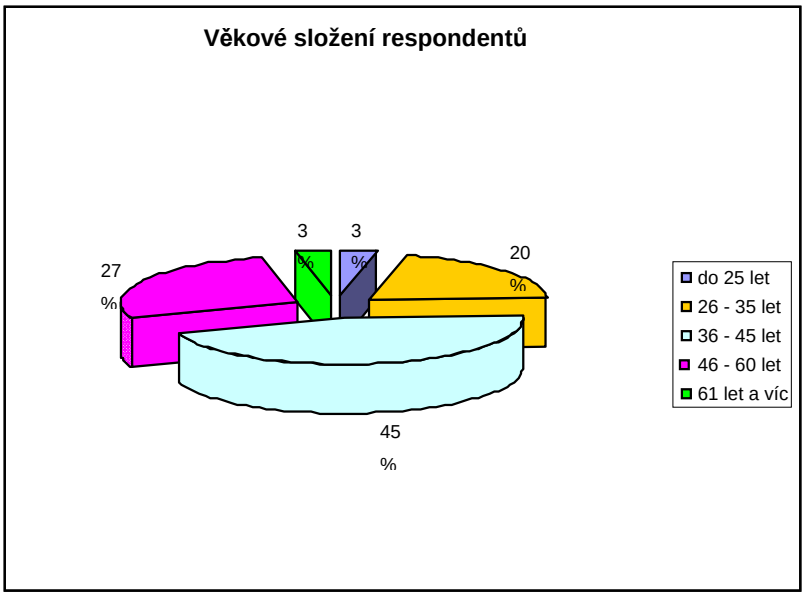


Obr. 8. Návrhy na zvýšení využitelnosti el.podatelen pro PO

Otázka č.9: Zařaďte se prosím do věkové kategorie.

Tab. 13. Vyhodnocení otázky č. 9

	Absolutní četnost	Relativní četnost
do 25 let	3	3%
26 - 35 let	18	20%
36 - 45 let	**40**	**45%**
46 - 60 let	24	27%
61 let a více	3	3%
celkem	88	100%



Obr. 9. Věkové složení respondentů

Otázka č.10: Jste muž, žena?

Tab. 14. Vyhodnocení otázky č. 10

	Absolutní četnost	Relativní četnost
muž	15	17%
žena	**73**	**83%**
celkem	88	100%

Dotazníkového průzkumu se zúčastnilo osmdesát osm zaměstnanců veřejné správy Olomouckého kraje všech věkových kategorií, z toho patnáct mužů (17%) a sedmdesát tři žen (83%).

Největší skupinu tvořili dotázaní ve věku 35 – 45 , a to 45%. Naopak nejméně tvořili 3% respondenti ve věku do 25 let a stejně tak respondenti starší 61 let jak ukazuje obrázek věkového složení respondentů (Obr. 9.).

Otázka č.11: Ve které instituci veřejné správy pracujete?

Tab. 15. Vyhodnocení otázky č. 11

	Absolutní četnost	Relativní četnost
krajský úřad	24	27%
městský úřad	**38**	**43%**
obecní úřad	0	0%
finanční úřad	18	20%
jiný úřad ne výše uvedený	8	9%
celkem	88	100%

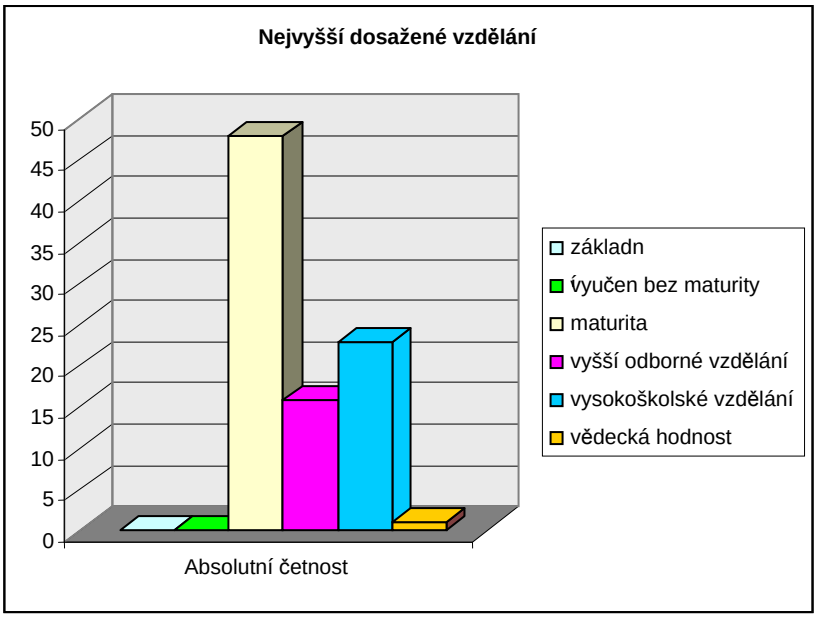
Nejvíce respondentů tvořili zaměstnanci městských úřadů, a to 43%. 27% dotázaných pracuje na Krajském úřadě v Olomouci, 20% oslovených je zaměstnanci některého z finančních úřadů Olomouckého kraje a 9% tvořili zaměstnanci jiného úřadu veřejné správy Olomouckého kraje, tedy nejsou zaměstnanci krajského, městského, obecního ani finančního úřadu. Šlo o zaměstnance Okresní správy sociálního zabezpečení Olomouc.

Otázka č.12: Nejvyšší dosažené vzdělání.

Tab. 16. Vyhodnocení otázky č. 12

	Absolutní četnost	**Relativní četnost**
základní	0	0%
vyučen bez maturity	0	0%
maturita	**48**	**55%**
vyšší odborné vzdělání	16	18%
vysokoškolské vzdělání	23	26%
vědecká hodnost	1	1%
celkem	88	100%

Jednou z otázek informativního charakteru byla i otázka č. 12. Zde jsem se ptala respondentů na jejich nejvyšší dosažené vzdělání. Nejnižší dosažené vzdělání účastníků dotazování byla maturita. Maturitním vzděláním se může pochlubit 55% oslovených. 18 % respondentů uvedlo jako své nejvyšší dosažené vzdělání vyšší odborné vzdělání, 26% účastníků průzkumu se pyšní vysokoškolským vzděláním a jeden dotázaný dokonce vědeckou hodností.



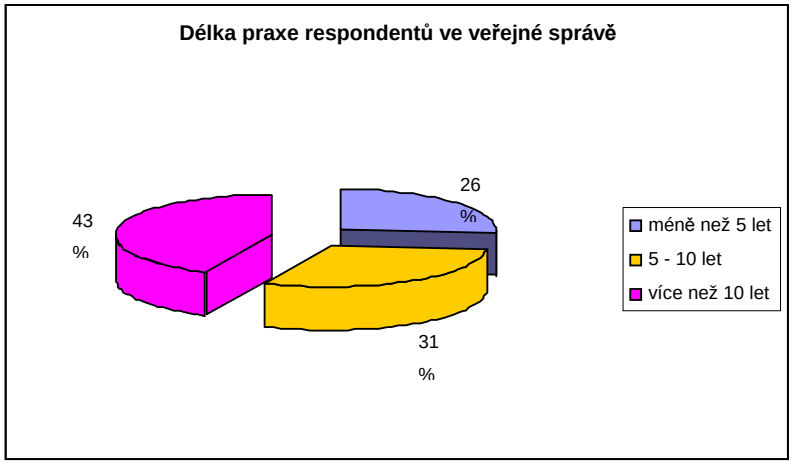
Obr. 10. Nejvyšší dosažené vzdělání

Otázka č.13: Jak dlouho pracujete ve veřejné správě?

Tab. 17. Vyhodnocení otázky č. 13

	Absolutní četnost	**Relativní četnost**
méně než 5 let	23	26%
5 - 10 let	27	31%
více než 10 let	**38**	43%
celkem	88	100%

Marketingové průzkumu se zúčastnilo 43% respondentů pracujících ve veřejné správě více než 10 let, 31% dotázaných uvedlo, že jsou zaměstnanci veřejné správy 5 – 10 let a 26% účastníků průzkumu pracuje ve veřejné správě méně jak 5 let.



Obr. 11. Délka praxe respondentů ve veřejné správě

9 SHRNUTÍ VÝSLEDKŮ MARKETINGOVÉHO VÝZKUMU

Průzkum probíhal v prvním čtvrtletí roku 2008 na 88 respondentech z celkových 120 oslovených. Návratnost dotazníku tedy činila 73%.

Navštívila jsem tyto instituce veřejné správy Olomouckého kraje:

- Krajský úřad Olomouc,
- Městský úřad Uničov,
- Městský úřad Šternberk,
- Městský úřad Litovel,
- Městský úřad Jeseník,
- Finanční úřad Šternberk,
- Finanční úřad Šumperk,
- Okresní správu sociálního zabezpečení Olomouc.

Návratnost dotazníků jednotlivých institucí veřejné správy Olomouckého kraje zobrazuje následující tabulka (Tab. 18.).

Tab. 18. Návratnost dotazníků

Oslovená instituce VS	**počet ks**	**z toho vráceno ks**	**návratnost v %**
Krajský úřad Olomouc	40	24	60%
Městský úřad Uničov	20	20	100%
Městský úřad Šternberk	10	7	70%
Městský úřad Litovel	5	5	100%
Městský úřad Jeseník	15	11	73%
Finanční úřad Šternberk	5	4	80%
Finanční úřad Šumperk	15	9	60%
OSSZ Olomouc	10	8	80%
celkem	**120**	**88**	**73%**

Dotazníky jsem rozdala respondentům a snažila se dohlížet na jejich správné vyplnění. Ve většině případů jsem se setkala s velkou ochotou a vstřícností ze strany zaměstnanců veřejné správy při vyplnění dotazníků. Našlo se pár jedinců, kteří dotazník nevyplnili, nešlo však ani tak o neochotu k jeho vyplnění, jako spíš o časovou zaneprázdněnost.

Při výzkumu byly používány primární informace získané přímo od jejich nositelů, tedy, zaměstnanců institucí veřejné správy Olomouckého kraje, prostřednictvím metody dotazování s využitím dotazníků (Příloha PI). V úvodní části dotazníku byl uveden cíl a důvod existence dotazníku, postup při jeho vyplňování, poděkování za vstřícný přístup respondentů k dotazníkům. Po zvážení různých typů otázek používaných při sestavování dotazníků byly zvoleny srozumitelně formulované uzavřené otázky s různou škálou nabízených odpovědí, v několika případech otázky polootevřené pro objasnění daného názoru respondenta, dále otázky výběrové trichotomické s uzavřeným koncem.

Použila jsem tedy otázky obsahové (otázky o mínění, postojích, orientaci a motivech chování) a po nich následují otázky informativního charakteru, které jsou zařazeny na konec dotazníku, neboť se jedná o údaje týkající se osobnosti respondenta. Jednotlivé otázky na sebe logicky navazují a je dodržen sled a stylizace.

Po uskutečnění dotazníkového šetření jsem analyzovala informace získané dotazníkovým šetřením.

Sběr se sestává ze samotného shromažďování dat. Získaná data jsem podrobila důkladnému rozboru a pomocí tabulkového procesoru Microsoft Excel jsem vypočítala ukazatele, které mě zajímaly.

Na závěr byly výsledky přehledně uspořádány do tabulek a grafů s připojeným textem a doporučením srozumitelně vysvětlujícím určitou situaci.

Po analýze dat získaných dotazníkovým průzkumem provedeným u vybraných institucí veřejné správy Olomouckého kraje jsem dospěla k závěru, že informovanost o problematice elektronického podpisu a elektronických podatelen, jejich možností využití při komunikaci s orgány veřejné správy, je u firem a především pak u občanů značně omezena. Proto navrhuji jako jedno z možných řešení větší medializaci tohoto problému formou spotů v rádiu či televizi. Další možností jak zvýšit využitelnost elektronické komunikace při komunikaci s orgány veřejné správy mohou být informační brožury, dostupné všem občanům a firmám, s jasnými pravidly a informacemi o možnostech využívání elektronického podpisu a postupech při podávání elektronických žádostí, přiznání a jiných formulářů prostřednictvím elektronických podatelen. Třetí možností jak dostat elektronický způsob komunikace s úřady do povědomí občanů a firem může být jejich oslovování pracovníky „fyzických“ podatelen.

Sami dotázaní, zaměstnanci institucí veřejné správy Olomouckého kraje, považují za největší výhodu využívání elektronického podpisu a elektronických podatelen právě úsporu času. Ten si uspoří nejen občané či firmy tím, že nebudou muset s každým formulářem osobně na příslušný, pošlou jej místo toho elektronicky, ale práce se zjednoduší i úředníkům, kteří již nebudou muset v takové míře čelit náporu a frontám lidí u přepážky.

Naopak největší nevýhodou z pohledu zaměstnanců veřejné správy Olomouckého kraje je právě neznalost dané problematiky soukromým sektorem, tudíž jak jsem již zmínila, je zapotřebí zvýšit informovanost společnosti.

ZÁVĚR

V této práci jsem se zabývala problematikou možností využívání elektronického podpisu při komunikaci s orgány veřejné správy, konkrétně s orgány veřejné správy Olomouckého kraje. Kromě samotného elektronického podpisu jsem se zaměřila i na využívání elektronických podatelen.

Cílem mé bakalářské práce bylo navrhnout doporučení k dalším možnostem využívání elektronického podpisu v institucích veřejné správy Olomouckého kraje, případně navrhnout doporučení ke zvýšení jeho využitelnosti.

V teoretické části jsem se zabývala vymezením pojmu elektronického podpisu, jeho legislativního rámce, elektronických podatelen, které spolu s elektronickým podpisem při komunikaci s veřejnou správou souvisí. Další část jsem věnovala základním pojmům, které jsou s elektronickým podpisem spojeny . A to například symetrické a asymetrické šifrování, certifikát, veřejný a soukromý klíč a mnoho dalších. K řešení úkolu v teoretické části jsem využila studia dané problematiky z literárních a elektronických zdrojů, které uvádím v seznamu použité literatury.

Praktická část je analýzou provedeného dotazníkového průzkumu a shrnutím zjištěných výsledků. Oslovením zaměstnanců veřejné správy Olomouckého kraje jsem se snažila zjistit využitelnost elektronického podpisu a elektronických podatelen při komunikaci s orgány veřejné správy, výhody a nevýhody této komunikace a doporučení k větší využitelnosti elektronického podpisu a elektronických podatelen.

SEZNAM POUŽITÉ LITERATURY

[1] Zákon č. 486/2004 Sb. úplné znění zákona č. 227/2000 Sb. o elektronickém podpisu.

[2] SMEJKAL, Vladimír. *Elektronický podpis jako nástroj pro zvýšení bezpečnosti informačních systémů*. 1.vyd. Brno : VITIUM, 2003. 30 s. ISNB: 80-214-2447-8.

[3] SMEJKAL, Vladimír. *Informační systémy veřejné správy ČR*. 1.vyd. Brno : Computer Press, 2004. 121 s. ISBN 80-245-0533-9.

[4] Elektronický podpis - důvěra ve světě informačních technologií. *Finanční noviny* [online]. 2006 [cit. 2008-05-13]. Dostupný z WWW: <http://www.financninoviny.cz/publicistika/index-view.php?id=183845>.

[5] BOSÁKOVÁ, D., KUČEROVÁ, A., PECA, P. *Elektronický podpis – překlad 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.

[6] *Informační systémy veřejné správy* [online]. 2001 [cit. 2008-05-13]. Dostupný z WWW: <http://www.isvs.cz/>. ISSN 1802-6575.

[7] *Kment Consulting* [online]. 2002-2006 [cit. 2008-05-13]. Dostupný z WWW: <http://www.vkc.cz/tema_ep_odkazy.htm>.

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

[9] *První certifikační autorita, a.s.* [online]. 2000 [cit. 2008-05-13]. Dostupný z WWW: <http://www.ica.cz>.

[10] DOSTÁLEK, L., VOHNOUTKOVÁ, M. *Velký průvodce PKI a technologií elektronického podpisu.* 1.vyd. Brno: Computer Press, 2006. 534 s. ISBN 80-251-0828-7.

[11] *SKYNET-Vaše bezpečná komunikace* [online]. 2008 [cit. 2008-05-13]. Dostupný z WWW: <http://www.pgp.cz/index.php?l=cz&p=7&r=4>.

[12] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat.* Brno : Computer Press, 2004. 190 s. ISBN 80-251-0106-1.

[13] Vyhláška č. 496/2004 Sb. k e-podatelnám.

[14] Nařízení vlády č. 495/2004 Sb. k e-podatelnám.

[15] STÁVKOVÁ, J., DUFEK, J. *Marketingový výzkum*. 1. vyd. Brno: MZLU v Brně, 2004. ISBN 80-7157-795-2.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA PI: DOTAZNÍK VYUŽITÝ PŘI MARKETINGOVÉM VÝZKUMU

Vážená paní, vážený pane,

dotazník, který Vám předkládám, se týká marketingového výzkumu postojů zaměstnanců institucí veřejné správy Olomouckého kraje k využívání elektronického podpisu a elektronických podatelen.

Dotazník je anonymní a získané informace budou sloužit pro potřeby průzkumu, který provádím v rámci své bakalářské práce na téma: „Možnosti využívání elektronického podpisu při komunikaci s orgány veřejné správy“ na Fakultě managementu a ekonomiky Univerzity Tomáše Bati ve Zlíně.

Pokud není uvedeno jinak, označte prosím jen jednu z uvedených odpovědí, která nejlépe vystihuje Váš postoj k dané problematice.

Velice Vám děkuji za Vaši ochotu a čas strávený nad tímto dotazníkem.

Veronika Vlčková

studentka 3.ročníku Fakulty managementu a ekonomiky

obor Hospodářská politika a správa

1. Využíváte elektronický podpis při své práci? (označte prosím křížkem)

ANO	*NE*

Pokud jej využíváte, jak často?(označte prosím křížkem)

- ☐ *spíše ne*
- ☐ *občas využívám*
- ☐ *často využívám*
- ☐ *využívám při každodenní práci*

2. Víte, co to elektronická podatelna je? (označte prosím křížkem)

ANO	*NE*

3. Má Váš úřad (Vaše organizace) zřízenou elektronickou podatelnu? (označte prosím křížkem)

ANO	*NE*

Pokud ANO, využívají ji spíše občané nebo firmy? (označte prosím křížkem)

- ☐ *spíše občané*
- ☐ *spíše firmy*
- ☐ *využívají občané i firmy*
- ☐ *nedokáži to posoudit*

4. Absolvovali jste specializovaná školení v oblasti elektronického podpisu nebo elektronické podatelny? (označte prosím křížkem)

ANO	*NE*

Pokud ANO, jaké oblasti se týkalo? (označte prosím křížkem)

- ☐ *pouze oblasti elektronického podpisu*
- ☐ *pouze oblasti elektronické podatelny*
- ☐ *oblasti elektronického podpisu i elektronické podatelny*

Pokud NE, měl byste zájem o absolvování těchto školení? (označte prosím křížkem)

- ☐ *zájem nemám*
- ☐ *zájem bych měl/a o elektronický podpis*
- ☐ *zájem bych měl/a o elektronickou podatelnu*
- ☐ *zájem bych měl/a o obojí*
- ☐ *momentálně nemám zájem, ale v budoucnu o tom uvažuji (budu to potřebovat ke své práci)*

5. V čem spatřujete výhody využívání elektronického podpisu? (můžete označit více možností)

- ☐ *Elektronická komunikace je bezpečnější při využití elektronického podpisu*
- ☐ *Úspora finančních prostředků při využití elektronického podpisu a elektronické podatelny*
- ☐ *Úspora času při využití elektronického podpisu*
- ☐ *Formulář (tiskopis) podepsaný elektronickým podpisem lze podat pomocí elektronické podatelny*
- ☐ *Nevím o žádné výhodě při využívání elektronického podpisu*
- ☐ *Jiné……*
  ……..

6. V čem naopak spatřujete nevýhody využívání elektronického podpisu? (můžete označit více možností)

- ☐ ***Složitost elektronického podpisu a obecně techniky pro zejména starší občany***
- ☐ ***Nutnost připojení k internetu, což je problémem zejména u občanů než institucí***
- ☐ ***Neznalost problematiky elektronického podpisu a elektronických podatelen sou-kromým sektorem***
- ☐ ***Nedůvěra v elektronickou komunikaci***
- ☐ ***Nevím o žádné nevýhodě při využívání elektronického podpisu***
- ☐ ***Jiné…….....***
  ……

7. Jaké cesty byste navrhovali pro zvýšení využitelnosti elektronických podatelen pro FO (fyzické osoby)? (můžete označit více možností)

- ☐ ***Oslovování občanů, kteří přijdou osobně na klasickou podatelnu***
- ☐ ***Informační brožury, letáky***
- ☐ ***Větší medializace***
- ☐ ***Jiné…….....***
  ……

8. Jaké cesty byste navrhovali pro zvýšení využitelnosti elektronických podatelen pro PO (právnické osoby)? (můžete označit více možností)

- ☐ ***Oslovování firem prostřednictvím dopisů či emailů***
- ☐ ***Informační brožury, letáky***
- ☐ ***Větší medializace***
- ☐ ***Jiné…….....***
  ……

9. Zařaďte se prosím do věkové kategorie. (označte prosím křížkem)

- ☐ ***do 25 let***
- ☐ ***26 – 35 let***
- ☐ ***35 – 45 let***
- ☐ ***46 – 60 let***
- ☐ ***61 let a více***

10. Jste ☐ ***muž*** ☐ ***žena*** ***(označte prosím křížkem)***

11. Ve které instituci veřejné správy pracujete? (označte prosím křížkem jednu možnost)

- ☐ ***Krajský úřad***
- ☐ ***Městský úřad***
- ☐ ***Obecní úřad***
- ☐ ***Finanční úřad***
- ☐ ***Jiný úřad kromě výše uvedených (správa soc.zabezpečení, zdravotní pojišťovny…)***

12. Nejvyšší dosažené vzdělání. (označte prosím křížkem)

- ☐ ***základní***
- ☐ ***vyučen bez maturity***
- ☐ ***maturita***
- ☐ ***vyšší odborné vzdělání***
- ☐ ***vysokoškolské vzdělání***
- ☐ ***vědecká hodnost (Ph.D., CSc.,…)***

13. Jak dlouho pracujete ve veřejné správě? (označte prosím křížkem)

- ☐ ***méně než 5 let***
- ☐ ***5 – 10 let***
- ☐ ***více než 10 let***

Ještě jednou Vám velice děkuji za trpělivost a poctivé vyplnění tohoto dotazníku.