Možnosti využívání elektronického podpisu při komunikaci s orgány veřejné správy

Veronika Vysloužilová

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 VYSLOUŽILOVÁ**
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 dostupné literatury charakterizujte problematiku elektronického podpisu.**

II. Praktická část

- **Proveďte analýzu současného stavu využívání elektronického podpisu v orgánech veřejné správy a ve vybraných společnostech na území města Otrokovice.**
- **Zhodnoťte výsledky provedené analýzy využívání elektronického podpisu.**
- **Navrhněte doporučení, jak zlepšit povědomí společností o využívání elektronického podpisu v praxi a jakým způsobem lépe informovat společnosti o možnostech aplikace elektronického podpisu v praxi.**

Závěr

*

Rozsah práce: **cca 40 stran**

Rozsah příloh:

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

Seznam odborné literatury:

[1] BOSÁKOVÁ, D. 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.
[2] JAŠEK, R. Informační a datová bezpečnost. 1. vyd. Zlín: Univerzita Tomáše Bati, 2006. 141 s. ISBN 80-7318-456-7.
[3] JAŠEK, R. Ochrana znalostí a dat v podnikových systémech. 1. vyd. Zlín: Univerzita Tomáše Bati, 2002. 115 s. ISBN 80-7318-095-2.
[4] ROSMAN, P., et al. Informatika pro ekonomy. 2. upr. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006. 233 s. ISBN 80-7318-430-3.

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.

doc. Dr. Ing. Drahomíra Pavelková
děkan

doc. RNDr. René Wokoun, CSc.
ředitel ústavu

ABSTRAKT

Bakalářská práce, která se zabývá možností využívání elektronického podpisu při komunikaci s orgány veřejné správy, si klade za cíl podat ucelenou informaci o elektronickém podpisu. Dále má za úkol zjistit současný stav využívání tohoto podpisu na území města Otrokovice a navrhnout způsob, jak zvýšit zájem o jeho využívání. Součástí této bakalářské práce je objasnění principů, na nichž je elektronický podpis založen a vysvětlení pojmů, které s touto problematikou souvisí. Zaměřuje se také na legislativní zakotvení elektronického podpisu, především v České republice.

Klíčová slova: elektronický podpis, asymetrická kryptografie, šifrování, časové razítko, certifikát, certifikační autorita, akreditace, e-podatelna

ABSTRACT

The bachelor thesis which deals with the possibilities of using a digital signature in the communication with public administration authorities proposes to give complete information about the digital signature. The next aim is to make out the present situation of using this signature at the urban area Otrokovice and to suggest the way how to increase the interest in using of the digital signature. One part of the thesis is the clearing of principles of the digital signature and there are explained the concepts connected with this theme. It also deals with the legislation of the digital signature especially in the Czech Republic.

Keywords: digital signature, asymetric cryptography, encryption, time stamp, certificate, certification authority, accreditation, electronic registry

Poděkování

Na tomto místě bych ráda poděkovala své vedoucí práce Ing. Miroslavě Dolejšové, Ph.D. za cenné rady a za čas, který mi věnovala.

OBSAH

ÚVOD

Dnešní doba je charakteristická dostupností velkého množství informací. Tato skutečnost vyžaduje potřebu naučit se tyto informace zpracovávat, třídit a správně je využívat. Vzdělávání se nyní stává celoživotní úlohou každého, kdo chce držet krok se současným vývojem. Je nedílnou součástí našich životů. Vzdělávání však vyžaduje i velké množství času a tak je snahou každého naučit se co nejlépe s časem hospodařit.

Fenoménem současné doby se stává Internet. Dříve lidé museli informace vyhledávat v knihách, nyní je většina informací zveřejněna na Internetu. Tam je lze nalézt mnohem rychleji a zároveň pohodlněji. Internet začíná pronikat prakticky do všech oborů a profesí. Možnosti jeho využití se zdají nevyčerpatelné. Odesílání pošty v podobě zalepené obálky či pohlednice mnohdy nahradila pošta elektronická. I vypisování formulářů na psacím stroji je již většinou minulostí a bylo nahrazeno formou elektronickou. Lidé dnes mohou trávit méně času ve frontách na úřadech. Některé záležitosti již mohou vyřizovat ze své kanceláře či přímo z pohodlí svého domova. Jednou z nových cest, která se před nedávnem otevřela,

a která může významně napomoci k urychlení vývoje v této oblasti, je i možnost používání elektronického podpisu. Tento podpis nahrazuje podpis psaný rukou a nevyžaduje tak fyzickou přítomnost osoby na místě předávání dokumentu.

A právě o využívání elektronického podpisu, především při komunikaci s orgány veřejné správy bude moje bakalářská práce.

Stanovení cílů v teoretické části

V první části své práce vysvětlím pojem elektronický podpis, objasním způsob jeho fungování i způsob jakým si můžeme tento podpis pořídit. Vysvětlím i některé další pojmy související s problematikou elektronického podpisu. Ve stručnosti uvedu zakotvení elektronického podpisu v zákonech.

Stanovení cílů v praktické části

Ve druhé části bakalářské práce provedu analýzu současného stavu využívání elektronického podpisu v některých orgánech veřejné správy a ve vybraných společnostech na území

města Otrokovice. Zhodnotím výsledky provedené analýzy. Zaměřím se i na názory a zkušenosti jednotlivých subjektů. V případě, že shledám využívání elektronického podpisu v tomto městě jako nedostatečné, pokusím se nalézt příčinu tohoto stavu a navrhnu doporučení, jak situaci zlepšit. Na základě získaných údajů navrhnu způsob jak zájem o využívání elektronického podpisu zvýšit. Pokud se ukáže, že je tento způsob komunikace již dostatečně rozšířený, rozeberu zkušenosti jednotlivých subjektů a budu hledat další možnosti na zlepšení jeho fungování.

Použitý způsob sběru a zpracování dat

Podklady pro analýzu jsem získávala několika způsoby. Nejčastěji jsem volila osobní návštěvu jednotlivých úřadů a firem, dále jsem se dotazovala telefonicky nebo jsem zasílala dotazníky konkrétním firmám, které se nacházejí na území Otrokovic, elektronickou cestou.

Jako metodu pro zpracování dat jsem si chtěla zvolit grafické znázornění a písemné zhodnocení výsledků. Vzhledem k výsledkům, které jsem v analýze získala, jsem však od grafického znázornění upustila.

I. TEORETICKÁ ČÁST

1 ELEKTRONICKÝ PODPIS

1.1 Vznik elektronického podpisu

Počátky elektronického podpisu je možné spojovat s elektronickou komunikací a tzv. e-obchodováním, kam patří jak obchod s hmotným i nehmotným zbožím jako je elektronika nebo hudební nahrávky, tak i obchod se službami, například informačními, právními a jinými. Elektronická komunikace i online prodej či poskytování služeb vyžaduje větší míru zabezpečení. Obvykle se totiž například uzavírání smluv o poskytování služeb neobešlo bez stvrzení vlastnoručním podpisem. Tím se zavazuji k plnění povinností, které mi ze smlouvy plynou a zároveň potvrzuji svou identitu, že jsem to byl skutečně já, kdo si danou službu objednal. Někdo si možná řekne, že podpis je poměrně snadno napodobitelný, ale není tomu tak. Díky odbornému grafologickému rozboru by mohlo být padělání jednoduše odhaleno. Vlastnoruční podpis je všeobecně považován za téměř nezpochybnitelný. Ve virtuálním světě je tomu ale jinak. Například naskenovaný podpis přiložený k odesílanému souboru nemůže být brán nikdy jako věrohodný. Proto bylo nutné řešit otázku, jak zajistit bezpečnější způsob identifikace osoby, se kterou komunikujeme. Pokud si uvědomíme, že osobu, se kterou uzavíráme například dohodu pouze elektronickou cestou, vlastně vůbec neznáme a že se s ní pravděpodobně ani nikdy nesetkáme, potřebujeme nutně prostředek, který nám umožní tuto osobu jednak identifikovat a následně i autentizovat. Identifikací rozumíme zjištění identity subjektu a autentizací zjišťujeme, zda je subjekt tím, za koho se prostřednictvím identity vydává. A protože nám v tomto případě nestačí běžně využívané prostředky jako je podpisový vzor, podpis ověřený matrikou ani telefonické ověření si osoby a obsahu zaslané zprávy, byl vyvinut prostředek nový a tím je elektronický a především zaručený elektronický podpis.

1.2 Legislativní zakotvení elektronických podpisů

Vznik elektronického podpisu můžeme spojovat se vznikem asymetrického šifrování. První zmínky bychom našly v sedmdesátých letech minulého století. Avšak k prvnímu právnímu zakotvení e-podpisu, jak ho známe nyní, došlo až v roce 1995, kdy byl v USA přijat první dokument zabývající se touto problematikou. Byl jím UTAH Digital Signature Act.

V Evropě se s prvním zákonem o elektronickém podpisu setkáváme v Německu, a to v roce 1997. Následovala Itálie, ale protože se brzy zjistilo, že podepsané dokumenty často

překračují národní úroveň, bylo třeba, aby se evropské státy dohodly na nějakém společném principu používání elektronických podpisů. Prvním výsledkem byl dokument vycházející z „Model Law on Electronic Commerce“ (modelový zákon o elektronickém obchodu – přijat v USA roku 1996). Následovala Směrnice Evropské Unie k elektronickému podpisu („Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures“), kterou předložila Evropská Komise ke schválení Evropskému parlamentu. Přijata byla 30.11.1999. Tato směrnice stanovuje právní rámec pro elektronické podpisy a některé certifikační služby. Směrnice byla formulována tak, aby byly naplněny tyto tři základní principy:

- technologická neutralita
- vydávání oprávnění pro poskytovatele certifikačních služeb není direktivně omezeno žádným schématem
- nezbytnost rozpoznání zákonné platnosti elektronických podpisů [14]

Členské státy měly nejpozději do 19. července 2001 uvést v účinnost právní a správní předpisy nezbytné pro dosažení souladu s touto směrnicí. Nejdůležitější ustanovení vnitrostátních právních předpisů pak měli sdělit Komisi. [22]

V návaznosti na Směrnici 1999/93/EC o elektronickém podpisu vznikla celá řada odborných skupin (Evropský ústav pro telekomunikační normy - ETSI, Evropská iniciativa pro normalizaci elektronických podpisů - EESSI a další). Jejich cílem bylo koordinovat standardizační aktivity tak, aby mohla být směrnice uvedena do praxe.

Později, a to v roce 2006, vydala Komise dokument, v němž vyjádřila své stanovisko, že cíle byly převážně splněny a že není potřeba tuto směrnici revidovat. Určité problémy se samozřejmě vyskytly. Používání elektronického podpisu se nerozvinulo v předpokládané míře a představa uživatele používajícího jediný digitální certifikát pro podpis, jenž by byl platný v celém elektronickém prostředí, se též nenaplnila.

1.3 Elektronický podpis v některých evropských státech

Směrnice 1999/93/EC je závazná pro evropské země. Její zásady měli členové unie dodržet i v národních právních úpravách. Na příkladu některých z nich, včetně legislativy v České republice, se můžeme podívat, do jaké míry se tohoto úkolu jednotlivé státy zhostily.

1.3.1 Česká republika

Česká republika na základě Směrnice 1999/93 přijala zákon č. 227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu). Přestože se na vypracování zákona o elektronickém podpisu pracovalo již před přijetím směrnice Evropské unie (EU), nebyl následný návrh schválen. Poté co byla přijata Směrnice 1999/93/EC bylo rozhodnuto, že se přizpůsobíme evropským normám.

V následující části uvedu stručný přehled právních předpisů, které upravují povinnosti a chování při elektronické komunikaci orgánů veřejné správy s občany (a naopak). S plným a aktuálním zněním všech těchto předpisů se lze seznámit například na stránkách Ministerstva vnitra.

Zákon č. 227/2000 Sb., o elektronickém podpisu upravuje v souladu s právem Evropských společenství používání elektronického podpisu, elektronické značky, poskytování certifikačních služeb a souvisejících služeb poskytovateli usazenými na území České republiky, kontrolu povinností stanovených tímto zákonem a sankce za porušení povinností stanovených tímto zákonem. Zatím poslední novela tohoto zákona nově zavádí pojem kvalifikované časové razítko a možnost používat tzv. elektronické značky.

Nařízení vlády č. 495/2004 Sb., o elektronickém podpisu stanoví povinnost orgánů veřejné moci zřídit e-podatelny (nebo v případě malého objemu elektronické komunikace zajistit příjem a odesílání zpráv prostřednictvím e-podatelny jiného úřadu). Dále ukládá povinnost vybavit příslušné zaměstnance zaručenými elektronickými podpisy a zajisti odpovídajícím způsobem ochranu zpracovávaných informací.

Vyhláška č. 496/2004 Sb., k elektronickým podatelnám stanoví postupy orgánů veřejné moci uplatňované při přijímání a odesílání datových zpráv prostřednictvím elektronické podatelny. Zároveň určuje strukturu údajů kvalifikovaného certifikátu, podle kterých je možné podepisující osobu při přijímání datových zpráv prostřednictvím elektronické podatelny jednoznačně identifikovat. Tato vyhláška navazuje na nařízení vlády č. 495/2004 Sb., k elektronickým podatelnám, které nařizuje orgánům veřejné moci elektronickou podatelnu zřídit a má sloužit jako návod, jak naplnit podmínky dané tímto nařízením vlády.

Vyhláška č. 366/2001 Sb. byla nahrazena vyhláškou 378/2006 Sb. Původní vyhláška stanovovala požadavky na celkovou bezpečnostní politiku a systémovou bezpečnostní politiku poskytovatelů certifikačních služeb vydávajících kvalifikované certifikáty a na krypto-

grafické moduly, které používají poskytovatelé vydávající kvalifikované certifikáty. Vyhláška 378/2006 Sb. o postupech kvalifikovaných poskytovatelů certifikačních služeb je určena těmto poskytovatelům a její první část obsahuje požadavky na jejich postupy při vydávání kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek.

Druhá část se vztahuje na označující osoby, zejména na orgány veřejné moci – obsahuje požadavky na ochranu soukromých klíčů, které se používají při vytváření elektronických značek.

První část vyhlášky nabyla účinnosti 17.8.2006, druhá část nabyla účinnosti 1.11.2006. [14]

Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů upravuje evidenci a kategorizaci archiválií, ochranu archiválií, práva a povinnosti vlastníků archiválií, využívání archiválií, zpracování osobních údajů pro účely archivnictví, soustavu archivů, práva a povinnosti zřizovatelů archivů, spisovou službu, která se vykonává písemnou formou nebo výpočetní technikou, působnost Ministerstva vnitra a dalších správních úřadů na úseku archivnictví a výkonu spisovné služby, správní delikty.

Zákon č. 101/2000 Sb., o ochraně osobních údajů v souladu s právem Evropských společenství, mezinárodními smlouvami, kterými je Česká republika vázána, a k naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí upravuje práva a povinnosti při zpracovávání osobních údajů a stanoví podmínky, za nichž se uskutečňuje předání osobních údajů do jiných států.

1.3.2 Velká Británie

Ve Velké Británii vstoupil v platnost 25.5.2000 zákon o elektronické komunikaci (Electronic Communication Act 2000). Tento zákon byl připravován již v době, kdy ještě nebyla schválena Směrnice 1999/93/ES o zásadách společenství pro elektronické podpisy. Tento zákon není plně v souladu s danou direktivou, definuje elektronickou komunikaci na mnohem širší a obecnější úrovni a v žádném případě neplní hlavní požadavek Směrnice – zrovnoprávnění elektronického podpisu s jeho písemnou formou. Směrnice 1999/93/EC byla implementována do britského právního řádu 8.3.2002 přijetím „The Electronic Signatures Regulations 2002“. [11]

1.3.3 Německo

Elektronický podpis je v Německu uzákoněn již od roku 1997. Zákon upravující základní podmínky elektronického podpisu a o změně některých dalších předpisů, který byl vydán k naplnění požadavků Směrnice, vstoupil v platnost 22.5.2001. Text zákona je jednotný, z pohledu požadavků Směrnice je úplný a především obsahuje kvalitní úpravu již zavedených principů elektronického podpisu. [11]

1.3.4 Itálie

V Itálii byl elektronický podpis upraven již roku 1997 předpisem č. 513. Ten byl nahrazen 26.1.2001 vyhláškou č. 445/2000 o elektronické komunikaci ve státní správě, která tak naplnila požadavky Směrnice Evropské unie pro elektronické podpisy. Kromě jiného upravuje používání časových razítek, zneplatnění a pozastavení platnosti certifikátů a také, velice účelně, nově definuje pojmy originál listiny a kopie. Velký význam se zde klade na reformu soudního informačního systému, který by měl umožňovat plně elektronickou komunikaci se soudy různé úrovně. [11]

1.4 Základní pojmy související s elektronickým podpisem

Celá problematika fungování elektronického podpisu je poměrně rozsáhlá a pro většinu uživatelů málo srozumitelná. Pro běžnou praxi není nezbytné znát přesně technické řešení elektronického podpisu, je však důležité umět se rozhodnout pro nejvhodnějšího poskytovatele a zvolit si správný typ podpisu. Pokud se chceme alespoň částečně seznámit s principem, na kterém elektronický podpis funguje, nevyhneme se takovým pojmům, jakými jsou kryptografie, asymetrické šifrování nebo hash funkce.

1.4.1 Kryptografie

Jedním ze základních pojmů, se kterými se při studiu elektronického podpisu setkáme, je kryptografie. Je to věda o šifrování dat za pomoci matematických metod. Šifrování je transformace dat do nečitelné podoby. Zpráva je pak pro osoby, jimž není určena, nesrozumitelná. Šifrování a dešifrování vyžaduje užití nějaké tajné informace, obvykle označované jako klíč. Tento klíč funguje podobně jako například klíče k domu a nepovoluje přístup neoprávněným osobám. [4]

Klíč se používá buď jeden pro zašifrování i dešifrování, pak jde o tzv. symetrické šifry.

Jinou možností je využití dvou klíčů, kdy jeden klíč slouží pro zašifrování a druhý klíč pro dešifrování. V tomto případě se jedná o asymetrické šifry. Říká se jim také šifry s veřejným klíčem. Šifrování slouží jednak k zakrytí obsahu přenášených informací, tak hrají důležitou roli v oblasti počítačové bezpečnosti.

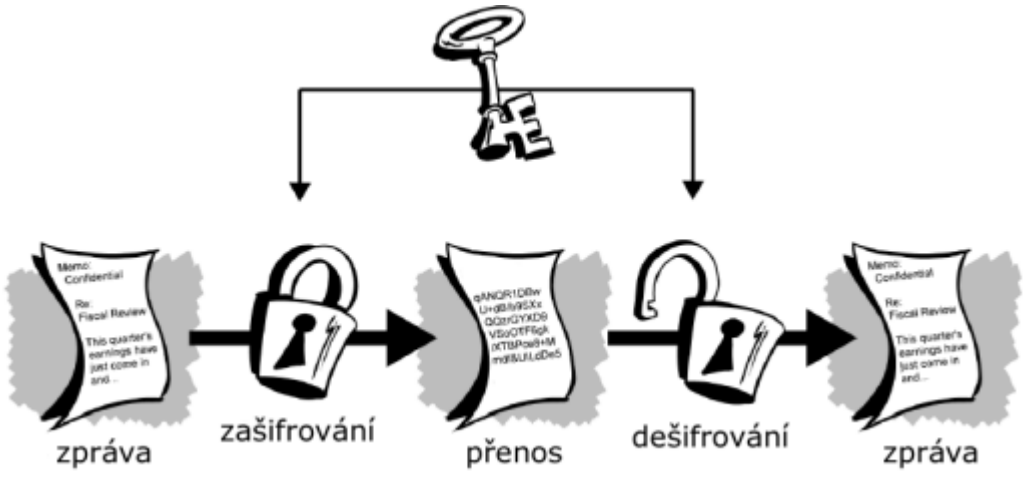
1.4.2 Symetrické šifrování

K zašifrování zprávy na straně odesílatele je použit stejný klíč, který je použit i na straně příjemce k dešifrování zprávy. Před začátkem komunikace musí být předán příjemci důvěryhodným kanálem šifrovací klíč, pomocí kterého pak může zprávu dešifrovat. Výhodou je, že symetrické šifrování je rychlé, nevýhodou pak, že při prozrazení klíče mohou být odkryta všechna data, která jím kdy byla zašifrována.

Mezi nejznámější symetrické šifrovací algoritmy patří např. DES (Data Encryption Standard). Byl vyvinut již v sedmdesátých letech minulého století. Používá klíč o délce 56 bitů. V současnosti se však používá jeho novější a bezpečnější verze 3DES (Triple – DES), která pracuje s klíčem dvojnásobným, dlouhým 112 bitů, případně s klíčem trojnásobným, dlouhým 168 bitů. Dalším příkladem je algoritmus IDEA s klíčem dlouhým 128 bitů.

V praxi se symetrické šifry využívají především pro zašifrování zálohových dat. [4]

Princip symetrického šifrování znázorňuje následující schéma (Obr. 1) na straně 16.



Obr. 1. Symetrické šifrování dat

Zdroj: [18]

1.4.3 Asymetrické šifrování

Asymetrické šifrování používá jiný klíč pro zašifrování zprávy, říká se mu veřejný klíč (public key) a jiný klíč pro dešifrování, ten nazýváme soukromý klíč (private key). Veřejný klíč je přístupný komukoliv, kdo chce šifrovaně odeslat data příjemci zpráv, naproti tomu soukromý klíč je tajný a proto musí být pečlivě chráněn. Ve skutečnosti jde o jeden klíč, který se při generování pomocí speciálního počítačového programu v následném kroku rozdělí na dvě části, vzájemně neodvoditelné. Tato vlastnost je velmi důležitá a tvoří podstatu bezpečnosti kryptosystémů s veřejným klíčem. Vzhledem k této vlastnosti je také složitější konstruovat takovéto šifrovací algoritmy. Důsledkem toho jsou tyto algoritmy při šifrování výrazně pomalejší. Oba klíče – veřejný a soukromý - pak spolu tvoří klíčový pár (key pair). [4]

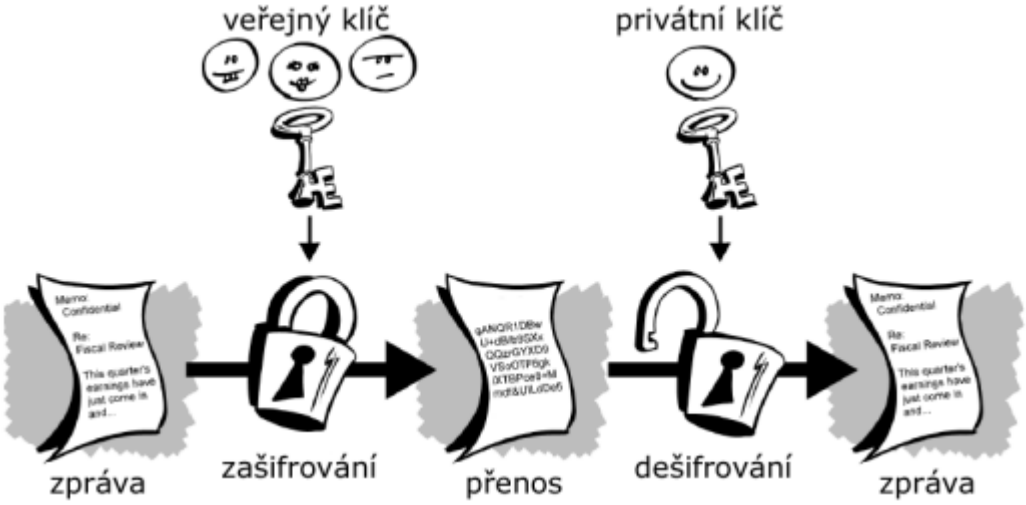
Některé kryptografické algoritmy mají takovou vlastnost, že je možné pro šifrování a dešifrování datových zpráv použít veřejného i privátního klíče. V tomto případě je možné tyto algoritmy použít i při realizaci elektronického podpisu. Uživatel, který chce ke své zprávě připojit elektronický podpis, použije k tomu svého privátního klíče. Každý, kdo zná jeho veřejný klíč může pomocí tohoto klíče ověřit připojený podpis a ví, že zprávu mohl odeslat pouze on, neboť vlastní příslušný privátní klíč.

Při podepisování datové zprávy jsou tedy klíče kryptoalgoritmu využity v obráceném pořadí než v procesu šifrování.

Šifrovací metoda RSA je zatím jedna z nejrozšířenějších a byla prvním známým algoritmem tohoto typu. Síla této šifry je založena na tom, že ještě neznáme rychlý způsob, jak rozložit velká čísla na prvočinitele. Pokud někdo objeví rychlý způsob rozložení velkých čísel na prvočinitele, bude šifra prolomena. Tato metoda byla zkonstruována v roce 1978. Využívá se pro distribuci klíčů pro symetrickou šifru, digitální podpisy, autentizaci atd.

Minimální spolehlivá délka klíče je 512 bitů, ale pro prostředí s vysokým utajením se doporučuje délka 2048 bitů.

Následující schéma znázorňuje princip asymetrického šifrování (Obr. 2).



Obr. 2. Asymetrické šifrování dat

Zdroj: [18]

1.4.4 Hash algoritmy

Pro pochopení fungování elektronického podpisu je vhodné seznámit se ještě s tzv. hash funkcí. Je to další oblast vedle šifrování symetrickým a asymetrickým klíčem. Využívá se v případě, že potřebujeme informaci pouze zašifrovat, ale už nikdy dešifrovat. Hash je v podstatě miniaturní otisk obsahu dokumentu. Vzniká pomocí funkce hash (hashing), která ze zadaného velkého množství dat vrací mnohem menší objem dat, který však jednoznačně vypovídá o obsahu dokumentu. Při změně jen jednoho bitu zprávy se musí hodnota hashe změnit. Doporučovaným standardem je délka hash funkce 160 bitů, která se používá i pro digitální podpisy. [4]

1.5 Princip fungování elektronického podpisu

Nejprve se odesílaný dokument (může to být textová zpráva, obrázek, počítačový program, databázový soubor - v podstatě vše, co v elektronické podobě existuje) převede tzv. hashovací funkcí do datového řetězce pevné délky, který jednoznačně charakterizuje text dokumentu. Tato hash hodnota se pak zašifruje pomocí asymetrické kryptografie soukromým klíčem podepisujícího. Výsledkem je pak elektronický podpis, který spolu s původním textem tvoří elektronicky podepsaný dokument. Příjemce dešifruje přijatý elektronický podpis veřejným klíčem podepisujícího, pak svými prostředky vypočte hash hodnotu dokumentu jednocestným hash algoritmem a srovná jej s hash hodnotou doku-

mentu, jehož šifra byla k dokumentu připojena. Pokud jsou obě hash hodnoty stejné, je dokument považován za autentický s nezměněným obsahem. [3]

Pokud komunikujeme s orgány veřejné zprávy, je nutné používat zaručený elektronický podpis.

1.6 Zaručený elektronický podpis

Existuje několik typů elektronického podpisu, ale protože se tato práce věnuje elektronickému podpisu při komunikaci s orgány veřejné správy, uvedu jen stručně jejich základní odlišnosti a budu se věnovat hlavně zaručenému elektronickému podpisu.

Hlavní rozdíl je ve splnění určitých požadavků. U některých typů není vyžadováno časové razítko a není definován žádný konkrétní formát nebo standard, který by popisoval tvar vytvořených nebo předávaných dat. Nebo není použit certifikát nebo jiný způsob zveřejnění pomocných dat (např. dat pro ověřování podpisu, osobních dat podepisující osoby, informace o systému použitém při podpisu). Tato pomocná data nejsou vůbec definována. Někdy ani nejsou kladeny žádné specifické požadavky na použitý podpisový systém nebo na prostředek pro vytváření, případně pro ověřování elektronického podpisu. Pak tento typ podpisu nemá pro příjemce příliš velkou vypovídací hodnotu a důvěra v něj je minimální. Slouží spíše pro informaci příjemce. Příkladem může být podpis vložený pod klasický e-mail. Skutečnost, že i tento podpis je podpisem ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu, vyplývá z § 3 odst. 1:

„Datová zpráva je podepsána, pokud je opatřena elektronickým podpisem.“ [1]

Z výčtu jednotlivých požadavků je pak zřejmé, že kategorie elektronických podpisů se budou lišit právě v těchto parametrech.

Zaručený elektronický podpis je takový 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 následující změnu dat. [4]

Jedinou dostupnou metodou elektronického podpisu je v současné době použití principu speciálního způsobu šifrové ochrany (kryptografie s veřejným a tajným klíčem, asymetrická kryptografie).

Moderní šifrování, neboli kryptografie je jedna z vyšších forem ochrany dat před nežádoucím přístupem k nim. Algoritmická ochrana dat spočívá v transformaci chráněných údajů do jiného nečitelného tvaru. [2]

1.7 Digitální certifikát, certifikační autorita a akreditace

Pokud chceme používat důvěryhodný elektronický podpis, bez digitálního certifikátu se neobejdeme. Zaručuje nejen získání soukromého klíče bezpečnou cestou, ale i zveřejnění našeho veřejného klíče a možnost vyhledat si veřejný klíč dalších osob, s nimiž chceme pomocí digitálního podpisu komunikovat. Na certifikátu jsou uvedeny údaje jako je veřejný klíč a identifikace subjektu. Dále obsahuje jedinečné sériové číslo certifikátu, dobu platnosti certifikátu, identifikaci vydavatele certifikátu a další.

Tyto certifikáty má oprávnění vydávat jen poskytovatel certifikačních služeb, označovaný jako certifikační autorita (CA). Může to být fyzická osoba, právnická osoba nebo organizační složka státu, která vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy. [5]

Pokud si chceme zřídit digitální certifikát budeme postupovat následovně:

- nejprve si sami pomocí dostupného softwarového vybavení vygenerujeme dvojici veřejného a soukromého klíče
- připravíme si osobní identifikační materiály nutné pro vydání certifikátu, např. IČO, DIČ, resp. číslo OP, rodné číslo, adresu elektronické pošty apod.
- certifikační autoritě předáme data pro vydání certifikátu spolu s doklady o jejich pravosti (většinou v podobě zprávy zašifrované veřejným klíčem certifikační autority)
- následně si certifikační autorita ověří pravost údajů (to znamená, že se dostavíme do sídla certifikační, případně registrační autority, kde předložením občanského průkazu a případných dalších identifikačních materiálů potvrdíme svou totožnost a pravost zaslaných dat)

- nyní vytvoří certifikační autorita digitální dokument s příslušnými informacemi, ten poté podepíše svým privátním klíčem a následně nám ho předá nebo po dohodě zašle

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

Pouze certifikační autorita akreditovaná Úřadem pro ochranu osobních údajů je jedinou autoritou, která je oprávněna vydávat certifikáty přijímané při komunikaci s orgány státní správy. [4]

Certifikační autorita může mít vytvořenu síť registračních autorit pro sběr údajů a informací.

Pojem akreditace ve smyslu zákona o elektronickém podpisu je osvědčení vydávané Úřadem pro ochranu osobních údajů poskytovatelům certifikačních služeb. Akreditovaný poskytovatel musí mít sídlo na území České republiky. Působení akreditovaných poskytovatelů je nezbytné v oblasti orgánů veřejné moci, neboť podle § 11 zákona:

„V oblasti orgánů veřejné moci je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydané akreditovanými poskytovateli certifikačních služeb“. [22]

Ministerstvo informatiky udělilo akreditaci k působení jako akreditovaný poskytovatel certifikačních služeb následujícím subjektům:

První certifikační autorita, a. s.

V oblasti kvalifikovaných certifikátů zahájila I. CA, a.s. poskytování certifikačních služeb již 18. 3. 2002 na základě akreditace udělené Úřadem pro ochranu osobních údajů. Ministerstvo informatiky ČR pak udělilo I. CA rozšířenou akreditaci pro výkon činnosti akreditovaného poskytovatele certifikačních služeb ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu a to s účinností od 1.2.2006. Prioritou I. CA je především komunikace v oblasti orgánů veřejné moci. Vydává jak komerční, tak kvalifikované certifikáty a po udělení rozšířené akreditace, je oprávněna poskytovat služby i v oblastech kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek. [15]

Rozdíl mezi certifikáty je především v ceně, škále možností jejich využití a také v míře zabezpečení.

V případě zájmu o kvalifikovaný certifikát ale počítejme s tím, že pokud využíváme více poštovních schránek (pro pracovní, soukromé či jiné účely) a všechny bychom měli rádi digitálně podepsané, musíme si zajistit samostatný certifikát na každou z nich. I. CA nabízí také uživatelům díky testovacímu certifikátu možnost vyzkoušet si elektronický podpis v bezplatné, čtrnáctidenní verzi. Tento certifikát „není uveden v seznamu použitých certifikátů, nemůže být zneplatněn a za jeho užití nenese I. CA žádnou zodpovědnost“. [7]

Služby tohoto poskytovatele certifikačních služeb využívají např.: Česká spořitelna, a. s.; ČSOB, a. s. nebo Eurotel, s. r. o. a další.

Česká pošta, s. p.

Česká pošta, s. p. se stala akreditovaným poskytovatelem certifikačních služeb 3. 8. 2005 na základě akreditace udělené Ministerstvem informatiky ČR. K vydávání digitálních certifikátů jsou pod Českou poštou s. p. celkem tři certifikační autority:

- Certifikační autorita – interní. Na interní bázi slouží v současné době výhradně pro vydávání certifikátů těm klientům, kteří mají s Českou poštu uzavřenou smlouvu o poskytování služeb a kteří v této smlouvě mají sjednáno předávání dat pomocí Internetu (e-mailem).

- Certifikační autorita – kvalifikovaná (QCA). Počínaje dnem 3.8.2005 se na základě rozhodnutí Ministerstva informatiky ČR stala Česká pošta, s. p. akreditovaným poskytovatelem certifikačních služeb ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu.

Provoz certifikační autority PostSignum QCA byl zahájen dne 1.9.2005. Fyzickým i právnickým osobám zajišťuje vydávání kvalifikovaných certifikátů a vydávání kvalifikovaných systémových certifikátů.

- Certifikační autorita – veřejná (VCA). PostSignum je nová elektronická služba České pošty, s.p. - služba Veřejné certifikační autority. Díky této službě můžeme za velmi příznivou cenu získat komerční certifikát, vhodný pro zabezpečení naší komunikace nebo citlivých dat (např. elektronické pošty). [9]

eIdentity a. s.

Společnost eIdentity a.s. provozuje následující certifikační autority:

- Akreditované služby. V oblasti orgánů veřejné moci a všude tam, kde je to požadováno zákonem či kde je nutné zajistit vysokou právní bezpečnost úkonů v elektronickém světě pomocí zaručeného elektronického podpisu, lze využít kvalifikovaný certifikát či kvalifikovaný systémový certifikát, který vydává Akreditovaná certifikační autorita eIdentity a.s. (ACAeID). Tato certifikační autorita získala akreditaci MIČR pro výkon činnosti akreditovaného poskytovatele certifikačních služeb v souladu se zákonem 227/2000 Sb. o elektronickém podpisu a vydává kvalifikované certifikáty pro použití pouze ve spojitosti s elektronickým podpisem.

- Komerční služby. Pro účely šifrování, identifikace, ale také pro vytváření a ověřování elektronických podpisů v oblasti běžné komerční komunikace lze využít elektronických certifikátů, vydaných Komerční certifikační autoritou (CCA). [10]

1.7.1 Způsob a cena pořízení certifikátu

O certifikát musí zájemce požádat elektronicky přes formuláře, které mají jednotlivé akreditované společnosti na svých internetových stránkách. Ideálně (v některých případech dokonce nutně) z počítače, na kterém bude žadatel elektronický podpis využívat. Většinou je poté nutné absolvovat jednu návštěvu pobočky příslušné certifikační společnosti. Mezi dokumenty, které bude certifikační společnost vyžadovat a kontrolovat, patří například výpis z obchodního rejstříku u právnické osoby, živnostenský list u fyzické osoby nebo potvrzení o zaměstnání.

Lhůtu, ve které musí akreditovaná společnost certifikát vydat, stát nijak nereguluje. Získání certifikátu od odeslání žádosti může být prakticky otázkou desítek minut.

Do velké míry záleží na klientovi, za jak dlouho certifikát získá. Po odeslání žádosti musí totiž například potvrdit smlouvu, zaplatit zálohovou platbu za službu, přijít na jednu asi 15 minutovou schůzku a nainstalovat si certifikát, což může každému trvat různě dlouho. Cestu od podání žádosti po instalaci certifikátu je možné urazit v průměru za tři dny. Často ale vychází akreditované společnosti klientovi vstříc a certifikát stihnou vydat v jednom dni. Drtivá většina certifikátů je však vydána přímo u klienta a na počkání za cca 1 hodinu.

Na jedné e-mailové adrese je možné, aby se podepisovalo více fyzických osob se svými kvalifikovanými certifikáty. V tomto případě by byla v kvalifikovaných certifikátech uve-

dena shodná e-mailová adresa. Pro tyto účely je však vhodnější používat kvalifikovaný certifikát, kde potřebná a chráněná data jsou uložena na čipové kartě. Potom uživatel může používat svou čipovou kartu k tvorbě svého elektronického podpisu všude tam, kde je k dispozici potřebná čtečka čipových karet.

Ceny služeb výše uvedených akreditovaných poskytovatelů jsou uvedeny mimo jiné na jejich webových stánkách. Ani ceny těchto služeb nejsou státem regulovány.

Jedná se řádově o několik set korun. Certifikát platí vždy jeden rok, a poté je ho třeba periodicky obnovovat. Tedy opakovaně hradit příslušný poplatek. [5]

1.7.2 Zneplatnění certifikátu

Každý certifikát, který nějaká certifikační autorita vydá, má pevně danou dobu platnosti (doba platnosti je uvedena přímo v každém certifikátu). Během doby platnosti certifikátu lze předčasně zrušit jeho platnost. Důvodem pro zneplatnění certifikátu může být například změna údajů o subjektu, kterému byl certifikát vydán nebo ztráta, popřípadě odcizení soukromého klíče držitele certifikátu. Tento soukromý klíč by pak mohl být zneužit cizí osobou, která by se mohla vydávat za skutečného majitele certifikátu. Každá certifikační autorita pravidelně vydává a zveřejňuje seznam zneplatněných certifikátů (CRL – Certifikate Revocation List), interval vydávání CRL je zpravidla 6, 12, 18 nebo 24 hodin. Většinou ji lze získat na webových stránkách příslušné certifikační autority.

2 ELEKTRONICKÁ PODATELNA

Elektronická podatelna je provozována na základě zákona č. 227/2000 Sb., o elektronickém podpisu, a jeho prováděcích předpisů.

Novela zákona o elektronickém podpisu stanoví, že orgány veřejné moci přijímají a odesílají datové zprávy opatřené uznávanými elektronickými podpisy prostřednictvím elektronických podatelen. Tuto povinnost upřesňuje s účinností od 1. ledna 2005 vyhláška č. 496/2004 Sb., o elektronických podatelnách. Při zřizování a provozování e-podatelen se orgány veřejné moci řídí rovněž nařízením vlády č. 495/2004 Sb., kterým se provádí zákon o elektronickém podpisu (účinnost rovněž od 1. ledna 2005). [5]

Elektronická podatelna tedy přijímá a dále zpracovává datové zprávy opatřené zaručeným elektronickým podpisem a doručené formou elektronické pošty (včetně příloh) na adresu, kterou si určuje sám orgán veřejné správy. Můžeme si ji vyhledat na webových stránkách jednotlivých úřadů, které mají e-podatelnu zřízenou. Doporučená maximální velikost zprávy je 10 MB. (Dokument je možné doručit i osobně, například na disketě.)

Formáty přijímaných souborů: doc, zip, xls, pdf, txt, rtf, gif, tif, jpeg.

Po přijetí podepsaného podání je provedena kontrola jeho elektronického podpisu a odesílateli je automaticky odeslána zpráva o výsledku kontroly podání a jeho přijetí nebo odmítnutí. Akceptovat lze pouze tzv. zaručený elektronický podpis opatřený kvalifikovaným certifikátem od akreditovaného poskytovatele certifikačních služeb. Podání je považováno za podepsané, je-li zaručeným elektronickým podpisem podepsané celé e-mailové podání nebo alespoň jedna z příloh. Pokud je elektronický podpis v pořádku, předá podatelna podání příslušnému úředníkovi k vyřízení.

Na zprávy nepodepsané, infikované virem nebo vyhodnocené jako spam není zpráva o doručení odesílána.

Pro e-mailovou komunikaci bez elektronického podpisu bývá v jednotlivých orgánech veřejné správy zřízena poštovní schránka s adresou odlišnou od adresy e-podatelny. Nepodepsané zprávy doručené na adresu elektronické podatelny jsou pak většinou automaticky předány do této schránky a je s nimi nakládáno jako s běžnou poštou.

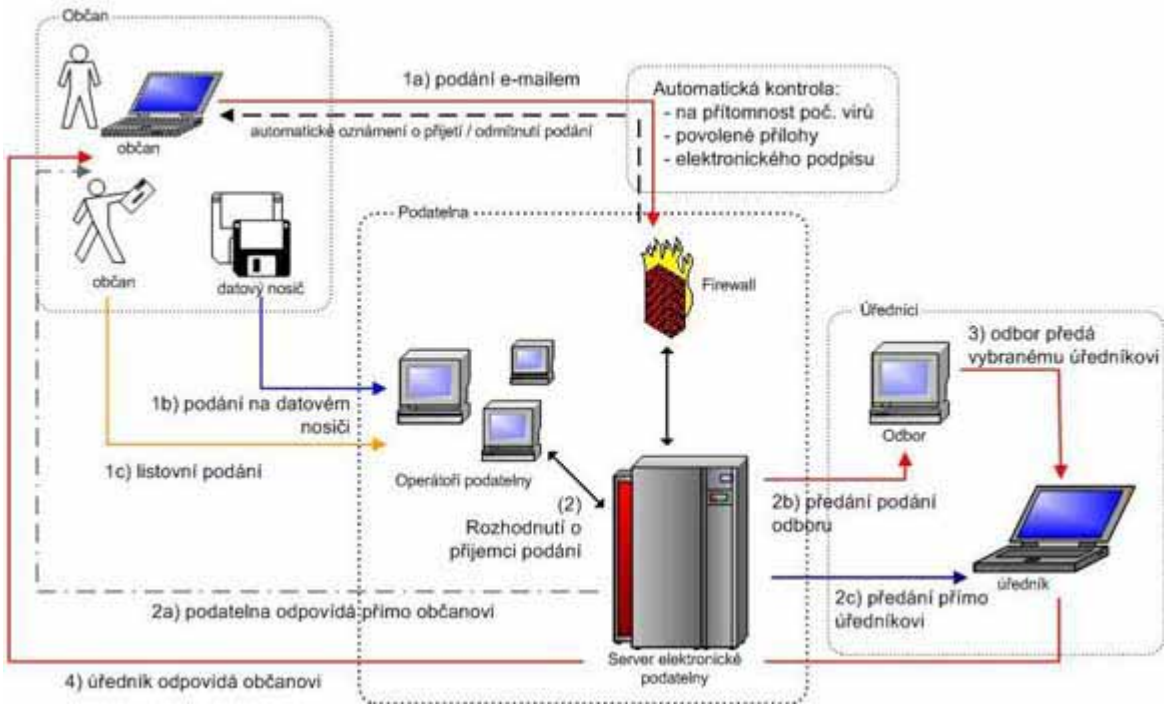
Elektronickou podatelnu (též „e-podatelnu“) tvoří souhrn technického vybavení, umožňující se připojit prostřednictvím sítě na elektronickou poštovní schránku podatelny, uložit a evidovat doručenou elektronickou poštu a postoupit ji k dalšímu vyřízení, dále obsluha e-podatelny a pravidla pro zacházení s elektronickými písemnostmi, nejčastěji ve formě spisového řádu a návodů pro obsluhu technického vybavení.

Obsluha e-podatelny musí také ověřit platnost elektronického podpisu a kvalifikovaného certifikátu, pokud jsou k doručené datové zprávě připojeny. [5]

2.1 Postup při zpracování doručené zprávy

V případě přijetí podání bez závad je odesilateli zaslána zpráva, která obsahuje: Potvrzení přijetí, PID - identifikační číslo podání, datum dokdy bude podání nejpozději vyřízeno. Zpráva bude podepsána elektronickým podpisem pracovníka podatelny úřadu, který zprávu přijal.

Na obrázku č. 3 - provoz podatelny - můžeme názorně vidět, jaké možnosti má pracovník podatelny při nakládání s podanou zprávou.



Obr. 3. Provoz podatelny

Zdroj: [19]

- Dle obsahu zprávy rozhodne operátor o předání podání k vyřízení některému z odborů, do jejichž referátu podání spadá. Předání je možné buď realizovat na centrální adresu odboru nebo v rámci něj vybrat konkrétního úředníka, který má vyřízení záležitosti ve svém referátu. Předáním bude zpráva odeslána na elektronickou adresu odboru nebo úředníka, která byla administrátorem nastavena. Předáním se automaticky přeposílají veškeré přílohy zprávy, data získaná z elektronického podpisu jsou uložena ve formátu HTML a tvoří jednu z příloh předané zprávy. V okamžiku předání se změní status zprávy na "ŘEŠENÁ".
- Pokud je obsah podání takový, že jej může vyřídit operátor podatelny, provede to formou odpovědi na zprávu. Jedná se zejména o žádosti o zaslání formulářů, dotazy ohledně běžného provozu úřadu, atd.. Aby nemusela obsluha podatelny zadávat stejné odpovědi vícekrát, existuje administrátorem spravovaná databáze Často pokládaných otázek (Frequently Asked Questions - FAQ). Operátor potom volí pouze jednu z předdefinovaných odpovědí, která se vkládá do těla zprávy. Po odeslání odpovědi se změní status zprávy na "VYŘÍZENÁ".
- V případě, že je přijatá zpráva obsluhou podatelny vyhodnocena jako mylná (jedná se typicky o spam) a není třeba odpovídat, je možné zprávu smazat, kliknutím na tlačítko Odstranit. Zpráva nebude smazána z databáze, ale bude jí přidělen příznak "SMAZANÁ". [19]

2.2 Kontrola stavu podání

Podávající má kdykoli možnost zjistit stav svého podání na stránkách úřadu.

Po vložení elektronické adresy, ze které bylo podání zasláno a identifikátoru PID je vygenerována historie konkrétního podání, včetně původní zprávy a odpovědi zaslané podatelnou nebo vyřizujícím úředníkem.

2.3 Vyřízení podání a archivace dat

Zpráva, která je předána k vyřízení, je doručena na předdefinovanou elektronickou adresu nebo má obsluha podatelny možnost vložit elektronickou adresu jinou (pro případ, že dotyčný úředník nebyl nalezen v připraveném seznamu). V okamžiku předání začíná běžet lhůta, v rámci které je očekávána odpověď od vyřizující strany. Příklad: Zákonná lhůta na

vyřízení podání je 30 kalendářních dní. Po 10 dnech je automaticky zasláno upozornění na adresu, kam se předávalo, že je očekávána odpověď. Pokud není, po dalších 10 dnech je zasláno upozornění na adresu, kam se předávalo a na adresu nadřízenou (vedoucí odboru). Pokud není zvolený odbor nebo úředník kompetentní k vyřízení předaného podání, na zprávu odpoví bez její modifikace s uvedením řetězce "NEVYRIZUJI" do Předmětu (subjectu) odpovědi. Takové podání přijde zpět na podatelnu s příznakem "NEVYŘÍZENO" a obsluha podatelny musí takové podání předat jiné kompetentní osobě. Pokud je zvolený odbor nebo úředník kompetentní k vyřízení předaného podání, odpoví na zaslanou zprávu, nemění ale obsah pole Předmět (subject) v odpovědi. Ke zprávě může přikládat libovolné přílohy a zpráva by měla být - dle povahy podání - elektronicky podepsána osobním zaručeným elektronickým podpisem vyřizujícího úředníka. Odeslaná zpráva projde podatelnou a bez dalšího zásahu obsluhy podatelny je poslána občanovi.

Data elektronické podatelny jsou archivována po dobu 5 let. [19]

2.4 Výhody a nevýhody elektronických podatelen

Elektronické podatelny můžeme považovat za výhodné především z hlediska občanů, kteří již nemusí docházet za každou maličkostí do kanceláří úředníků, ale mohou si záležitosti vyřídit přes svůj počítač a internet stáhnutím příslušného formuláře a zasláním emailu. Výhodou je i to, že e-podatelny fungují nonstop. Téměř odpadne chození na úřad, sledování nervózních pohledů úředníků a kontrola času, kvůli úředním hodinám. Využití e-podatelen je výhodné i pro pracovníky úřadů, protože mohou řešit jednotlivé případy ve stanovených časových lhůtách a v klidu. Další výhodou je, zvláště pak v případě, že je dokument zaslán elektronicky na předepsaném formuláři, že odpadá zbytečné a zdlouhavé přepisování dat z formulářů přinesených jen v tištěné formě.

Nevýhodou e-podatelen jsou především vysoké náklady při jejich zřizování. K těmto nákladům patří nákup hardwaru a softwaru, zajištění elektronického podpisu pomocí kvalifikovaného certifikátu vydaného akreditovaným poskytovatelem certifikačních služeb či zaučení úředníků obsluhující tyto e-podatelny.

3 ČASOVÉ RAZÍTKO A ELEKTRONICKÁ ZNAČKA

Časovým razítkem je datová zpráva, kterou vydal 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.

Časové razítko slouží k „orazítkování“ dokumentu, u kterého požadujeme důkaz, že v daném čase v této podobě existoval. Na základě požadavku tento dokument orazítkuje autorita časových razítek. Časové razítko obsahuje především aktuální datum a čas, číslo časového razítka a identifikaci poskytovatele, který toto razítko vydal. Tyto údaje se připojí ke vstupním datům a vše se opatří elektronickým podpisem autority časových razítek. Celek se pak zašle žadateli jako odpověď na jeho žádost. [5]

V řadě případů nestačí mít pouze digitálně podepsaný dokument. Zvláště u dokumentů s relativně dlouhou dobou platnosti (např. smlouva o půjčce) je možné, že bude jedna ze stran chtít zpochybnit platnost dokumentu, který podepsaly obě strany. Není nic snazšího než nahlásit ztrátu privátního klíče a nechat odvolat certifikát. Bez existence časového razítka daného dokumentu již nikdo nedokáže, zda byl dokument podepsán před tímto odvoláním nebo až po něm.

Čas odvozený ze systémového času počítače není důvěryhodný, protože je snadné ho změnit.

Časové razítko tedy především zajišťuje důkaz o existenci dokumentu v daném čase .

Existence Autority časových razítek (Time Stamping Authority TSA) je také nutným základem pro poskytování elektronických notářských služeb a zajištění dlouhodobé archivace elektronicky podepsaných dokumentů.

Je nutné uvědomit si, že časové razítko neobsahuje identifikaci žadatele, což znamená, že nemůže sloužit jako důkaz o tom, že bezprostředně před okamžikem vydání razítka měla dokument v držení určitá osoba. [6]

Elektronická značka je z technologického hlediska stejná jako zaručený elektronický podpis, tj. jedná se o digitální podpis. Pro vlastní vytváření elektronických značek nebo pro přijímání datových zpráv jimi označených není tedy potřeba pořizovat jiný software.

Odlišnost elektronické značky a zaručeného elektronického podpisu má především právní charakter. Elektronický podpis vytváří fyzická osoba (stejně jako vlastnoruční), elektronickou značkou může datové zprávy označovat i právnická osoba nebo organizační složka státu. Lze ji přirovnat k otisku úředního razítka.

Použití elektronické značky urychlí vydávání některých dokumentů, protože značkami budou tyto dokumenty moci být opatřovány automatizovaně, bez nutnosti ověření obsahu každé označované datové zprávy. Předpokladem je samozřejmě zadání náležitých parametrů vydávaných datových zpráv a odpovídající bezpečnostní opatření. [5]

II. PRAKTICKÁ ČÁST

4 ÚVOD K PRAKTICKÉ ČÁSTI

Téma bakalářské práce „Možnosti využívání elektronického podpisu při komunikaci s orgány veřejné správy“ jsem si zvolila i z praktického důvodu. Pracovala jsem v soukromé firmě v Otrokovicích, kde jsem měla na starosti také komunikaci s orgány veřejné správy. Tato práce obnášela vypisování různých formulářů, jejich přeprava na jednotlivé úřady, kde byly většinou jen opatřeny razítkem a následná cesta zpět. Vzhledem k tomu, že sídlo firmy se neshodovalo se sídlem provozovny, bylo nutné jezdit několikrát měsíčně až do 15 km vzdáleného města. Často se stávalo, že docházelo ke značným časovým ztrátám. O možnosti zasílat dokumenty v elektronické podobě a využívat e-podpis mě ani ve firmě ani na žádném úřadě nikdo neinformoval. Na tuto problematiku jsem narazila až při studiu ve škole a protože jsem chtěla znát bližší informace a také získat názory firem a orgánů veřejné správy na využívání elektronické podpisu v praxi, zvolila jsem si právě toto téma. Výsledky chci zhodnotit a případně navrhnout zaměstnavateli, abychom zavedli tento způsob komunikace s úřady i do naší firmy.

Dále se pokusím navrhnout doporučení, jak zlepšit povědomí společností o využívání elektronického podpisu v praxi.

4.1 Jak si obstarat e-podpis na území města Otrokovice

Na území města Otrokovice se nachází jedna pobočka registrační autority I.CA pro vydávání komerčních i kvalifikovaných certifikátů I.CA. Pracoviště je umístěno na pobočce Československé obchodní banky, a.s. Žádost o certifikát lze podle návodu na internetových stránkách vyplnit a odeslat z vlastního počítače, pak je nutné navštívit pobočku a provést identifikaci. Celý postup je uveden v teoretické části bakalářské práce. Při potížích je možné využívat zvláštní e-mailovou adresu zřízenou právě k tomuto účelu. Pokud bychom měli zájem o školení v oblasti využívání elektronického podpisu, může ho pro nás I.CA realizovat v rámci vydání certifikátu v naší společnosti.

Dalšího akreditovaného poskytovatele certifikačních služeb Českou poštu, s. p. musí zájemce navštívit například ve Zlíně. V případě, že se obrací na poštu v Otrokovicích, nejsou mu poskytnuty žádné bližší informace. Je pouze odkázán na návštěvu hlavní pošty ve Zlíně. Četnost dotazů na možnost získání e-podpisu na Otrokovické poště je nevelká. Pouze několik tazatelů za měsíc.

Společnost eIdentity a.s., která má také akreditaci k působení jako akreditovaný poskytovatel certifikačních služeb, provozuje v současné době jedno pevné registrační místo na adrese sídla společnosti, což je v Praze. Další registrační místa jsou mobilní a mohou poskytovat své služby po domluvě dle požadavků zákazníka.

5 PORTÁL VEŘEJNÉ SPRÁVY

Pokud se chceme seznámit s problematikou veřejné správy, je Portál veřejné správy jedním z nejvhodnějších zdrojů informací. Tento portál poskytuje službu občanům a organizacím a pracuje na vybudování celého systému elektronické veřejné správy. Soustřeďuje zde informace o úřadech státní správy i samosprávy, zajišťuje bezplatný přístup k informacím a službám veřejné správy a poskytuje například i návody, jak postupovat v různých životních situacích. Hlavní části portálu obsahují kompletní adresář veřejné správy, odkazy na zákony, které se týkají řešeného problému, elektronický Obchodní věstník, poskytuje i náhled do katastru nemovitostí, můžeme si zde vyhledat potřebné formuláře. Součástí portálu jsou i zprávy a noviny z oblasti veřejné správy nebo přehled veřejných zakázek. Z hlediska problematiky, kterou řeší tato bakalářská práce, je významný oddíl s názvem Podání, kde se seznámíme s dostupnými službami právě v aplikaci elektronického podání. Slouží i pro registraci uživatelů, kteří chtějí komunikovat s veřejnou správou elektronicky.

V současné době jsou na Portálu veřejné správy v aplikaci Elektronická podání dostupné následující služby:

a) Služby České správy sociálního zabezpečení

- Evidenční listy důchodového pojišťění (ELDP)

- Přihlášky zaměstnanců k nemocenskému pojištění, odhlášky (P/O)

- Přehled o příjmech a výdajích OSVČ

b) Služby Ministerstva průmyslu a obchodu

- Roční výkaz o poštovních službách PS (MI)1-01

c) Služby Ministerstva financí

Česká daňová správa umožňuje daňovým subjektům podávat daňové přiznání a další písemnosti v elektronické podobě. Elektronické podání pro daňovou správu nabízí v současnosti zpracování následujících písemností:

- Daňové přiznání z příjmu fyzických osob typ A a B

- Daňové přiznání z příjmu právnických osob

- Přiznání k dani z přidané hodnoty

- Daňové přiznání k dani silniční

- Daňové přiznání k dani z nemovitostí

- Oznámení o nezdaněných vyplacených částkách fyzickým osobám

- Obecná písemnost

d) Služby Generálního ředitelství cel

Celní správa-Intrastat - systém zajišťující sběr dat pro statistiku obchodu se zbožím mezi členskými státy EU.

Elektronické podání daňových přiznání ke spotřebním daním.

e) Ministerstvo dopravy

Ministerstvo dopravy provozuje systém eTesty sběr výsledků zkoušek uchazečů o řidičské oprávnění provedených elektronicky.

f) Ministerstvo životního prostředí - Centrální ohlašovna znečištění

Centrální ohlašovna je informační systém shromažďující ohlašované údaje z oblasti životního prostředí. Slouží současně jak ohlašujícím subjektům (nejčastěji zemědělské a průmyslové podniky), tak orgánům státní správy pověřeným kontrolou, evidencí a zpracováním ohlášených údajů (např. Česká inspekce životního prostředí, krajské úřady, obce, magistráty, správci povodí a další). [20]

6 ORGÁNY VEŘEJNÉ SPRÁVY NA ÚZEMÍ MĚSTA OTROKOVICE

6.1 Městský úřad Otrokovice

Městský úřad Otrokovice má zřízenu e-podatelnu, která je určena pro příjem podání učiněných v elektronické podobě opatřených i neopatřených zaručeným elektronickým podpisem (dále jen"písemnost"). Písemnosti přijaté prostřednictvím elektronické podatelny a splňující předepsané náležitosti úřad vyřizuje stejnými postupy a ve stejných lhůtách jako podání neelektronická.

Příjem písemností na adrese elektronické podatelny (epodatelna@muotrokovice.cz) probíhá automatizovaně celých 24 hod. U každé písemnosti je zaznamenán čas a datum, kdy byla písemnost přijata. Okamžitě po odeslání písemnosti obdržíme potvrzení o přijetí. Maximálně do příštího pracovního dne obdržíme další email s číslem jednacím, které bylo přiděleno naší písemnosti. U přijaté písemnosti, které nevyžadují odpověď (nabídky, reklamy), neobdržíme číslo jednací. Ve stanovené lhůtě od podání písemnosti obdržíme odpověď úřadu. [16]

Informace o využívání elektronické komunikace, za použití elektronického podpisu, s Městským úřadem v Otrokovicích mi poskytla přímo pracovnice e-podatelny. Tento způsob komunikace využívá jen několik firem, které si elektronický podpis zřídily a využívají ho opakovaně. Další uživatelé přibývají jen velmi málo. Zájem víceméně stagnuje.

Přesný důvod, proč je zájemců tak málo nezná, ale předpokládá, že jím bude jednak určitá složitost při zahájení využívání tohoto způsobu komunikace, tak určitá konzervativnost občanů a firem. Dále to může být především i potřeba většinu problematik prodiskutovat s pracovníky úřadu.

Kromě již zmíněných názorů bych přidala i jeden vlastní postřeh. Při návštěvě stránek Městského úřadu Otrokovice a konkrétně stránky e-podatelna jsem postrádala bližší informace, co vše je možné na e-podatelnu zasílat. Nebyly zde žádné odkazy na postup nebo podmínky, za jakých lze elektronickou komunikaci uskutečňovat, ani odkazy na případné formuláře. Při srovnání s jinými portály veřejné správy, které mají tento projekt pečlivě zpracován, na stránkách e-podatelny tohoto městského úřadu zájemce nezjistí téměř nic.

6.2 Zdravotní pojišťovny

Než jsem se zaměřila na konkrétní pobočky zdravotních pojišťoven na území Otrokovic a na jejich zkušenosti s využíváním elektronického podpisu, zjistila jsem si, co vše je v současné době možné elektronicky na pojišťovny zasílat.

Portál zdravotních pojišťoven

Například na Portálu ZP, který je internetovou aplikací vytvořenou pro zlepšení a zrychlení komunikace mezi pojišťovnami provozujícími tento Portál ZP (Česká národní zdravotní pojišťovna, Oborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví, Revírní bratrská pokladna, zdravotní pojišťovna, Vojenská zdravotní pojišťovna České republiky, Zaměstnanecká pojišťovna Škoda, Zdravotní pojišťovna Metal-Aliance) a poskytovateli zdravotní péče, plátci pojistného i samotnými pojištěnci, jsem zjistila, že umožňuje automatizovaný přístup při výměně dat typu: předávání dávek a faktur, hromadné oznámení zaměstnavatele, přehled plateb zaměstnavatele, elektronická podatelna. [21]

Hutnická zaměstnanecká pojišťovna – elektronická přepážka

Na Elektronické přepážce této pojišťovny, což je moderní internetová aplikace přinášející změnu ve vzájemné komunikaci klienta a pojišťovny, jsem si zjistila, že ji lze využít pro vyúčtování zdravotní péče, výpis faktur, výpis plateb, ověření příslušnosti pojištěnce k HZP, žádost o přehled kapitovaných pojištěnců (zdravotnická zařízení), hromadné oznámení zaměstnavatele, zasílání přehledu platbě pojistného, požadavek na seznam zaměstnanců (zaměstnavatelé), výdajový účet pojištěnce, změna kontaktních údajů, záznam o dlouhodobém pobytu v cizině, změna údajů o plátci, žádost o nový průkaz, vyúčtování pojistného pro OSVČ (pojištěnci). [12]

Prostřednictvím osobního certifikátu nebo SMS kódu můžeme 24 hodin denně, 7 dní v týdnu, provádět v klidu svého domova nebo kanceláře všechny základní operace, kvůli kterým již nemusíme chodit na pobočky HZP.

Portál Všeobecné zdravotní pojišťovny ČR

Všeobecná zdravotní pojišťovna České republiky nabízí svým pojištěncům, smluvním partnerům, zaměstnavatelům i státním institucím, vlastnícím příslušné certifikáty, zdarma přístup na svůj Portál. Portál VZP ČR nabízí bezpečnou výměnu digitálně podepsaných dat a poskytování informací z informačního systému VZP ČR.

Přínos Portálu ocení především klienti, kteří pravidelně komunikují s VZP ČR.

Služby, které nabízí prostřednictvím elektronické komunikace:

Poskytovatelům zdravotní péče:

- ověření aktuální registrace pojištěnce u zdravotní pojišťovny
- ověření platnosti smlouvy s VZP ČR
- vyhledání zdravotnického zařízení ve smluvním vztahu k VZP ČR
- vyhledání informace o registraci pojištěnce u jeho ošetřujícího lékaře
- zasílání faktur za poskytnutou zdravotní péči
- předávání souborů vyúčtování zdravotní péče poskytnuté pojištěncům VZP ČR

Zaměstnavatelům:

- zpracování hlášení a kontrolu identifikačních údajů zaměstnavatele
- zpracování a zaslání hlášení hromadného oznámení zaměstnavatele
- zaslání přehledu o platbě pojistného na zdravotní pojištění zaměstnavatele
- informování zaměstnavatele o jeho platbách pojistného
- podávat Oznámení o změnách v evidenci zaměstnavatele

Osobám samostatně výdělečně činným:

- zasílat Přehled o příjmech a výdajích za příslušný rok
- zasílat vyúčtování plateb pojistného a přehled o platbách pojistného a penále

Pojištěncům:

- podávat Oznámení pojištěnce
- požádat o zaslání Přehledu vykázané zdravotní péče na pojištěnce
- reklamovat Přehled vykázané zdravotní péče na pojištěnce

Státním institucím:

- podávat hromadná oznámení

Jeho velkou výhodou je zjednodušení administrativy, zrychlení komunikace klientů s pojišťovnou a v neposlední míře i značná úspora času. [23]

Z tohoto výčtu je zřejmé, že Všeobecná zdravotní pojišťovna nabízí největší rozsah služeb spojený s elektronickou komunikací a na jeho portále je opravdu propracovaný systém, který vysvětlí zájemci vše potřebné, aby mohl používat tento způsob komunikace.

6.2.1 VZP - Úřadovna Otrokovice a HZP – expozitura Otrokovice

Informace o využívání elektronického podpisu mi poskytly pracovnice těchto úřadoven. Záměrně jsem tyto informace spojila do jednoho odstavce, protože se v obou případech téměř shodovaly.

Pracovnice věděly, že existuje možnost podávat hromadná oznámení, přehledy a jiné dokumenty elektronickou cestou s využitím elektronického podpisu, ale sdělily mi, že se na těchto pracovištích nevyužívá. Mají informace, že existuje jedna celostátní centrála, která tyto elektronicky podepsané formuláře přijímá a následně je rozesílá na pracoviště jednotlivých poboček, kde se zpracovávají. Zájem o poskytnutí informací o možnosti využívat elektronickou cestu k doručování dokumentů je, podle jejich vyjádření, téměř nulový. V případě, že se někdo o tuto problematiku zajímá, odkáže ho pracovnice většinou na webové stránky příslušné zdravotní pojišťovny, kde si může podrobné instrukce přečíst nebo na telefonickou konzultaci z někým z centrály. U VZP může pracovnice zájemce odkázat na pobočku ve Zlíně, kde je možná registrace a podpis smlouvy o využívání elektronické komunikace. Žádnou jinou praktickou pomoc ve formě instrukcí, vysvětlení postupných kroků nebo vyhledávání formulářů pracovnice neposkytují.

Žádné statistické údaje o využívání elektronické komunikace se zdravotními pojišťovnami na těchto pobočkách nemají. Věděly pouze o jedné lékařce z Otrokovic, která tuto formu zasílání dokumentů využívá.

6.3 Finanční úřad

Při jednání na FÚ v Otrokovicích jsem požádala o informace vedoucí pracovnici. Elektronický podpis a obecně elektronickou komunikaci mezi úřadem a občanem a mezi úřady

vzájemně považuje za velmi přínosné. Se vzrůstajícím zájmem ze strany poplatníků předpokládá i významný ekonomický efekt.

Tento způsob předávání dat je ale zatím ze strany občanů a organizací jen málo využívanou cestou. I když jsou pracovnice finančního úřadu školeny, aby dokázaly vysvětlit základní princip fungování elektronické komunikace a sami by také uvítaly, kdyby především větší společnosti na tuto formu komunikace přešly, přesto se počet uživatelů počítá jen na desítky. Jen velmi málo firem si elektronický podpis zřídilo a dále se připojilo k využívání
e-podatelny zřízené k tomuto účelu. Když jsem požádala o přesnější informace, odpověď byla opravdu alarmující. Z doručených asi 10 000 dokumentů je jich zhruba jen 20 – 30 zasláno elektronicky. Tuto skutečnost jen potvrzuje následující zpráva, která se týká celé České republiky:

Zájem o jeho využívání sice roste, ale nijak závratně. Loni je k přiznání daně z příjmu využilo deset tisíc uživatelů, a to dohromady jak z řad firem a podnikatelů, tak i zaměstnanců. Finanční úřady však celkem zpracují 2,5 milionu přiznání, takže bez papíru nejde ani o jedno procento. [17]

Valná většina dokumentů je předávána přímo na pobočce a je vyplněna buď perem nebo v počítači na předepsaném formuláři, ale vytištěna, což znamená, že pracovnice musí údaje znovu přepsat do počítače, do programu, který je určen pro jejich zpracování. Je to jistě zbytečná ztráta času i financí vynaložených na tuto činnost. Ta je pak vlastně zaplacena dvakrát. Jednou poplatníkem a jednou finančním úřadem.

I přesto, že podrobné informace o možnosti přechodu na elektronickou komunikaci s FÚ jsou uvedeny na webových stránkách Ministerstva financí a je možné seznámit se s nimi na nástěnce v budově finančního úřadu a také pracovnice úřadu se snaží přesvědčit firmy, aby přešly na tuto formu komunikace, pasivita poplatníků stále převažuje. Jako důvod uvádějí, že jim stávající způsob vyhovuje, že to na úřad nemají daleko, že tam nejezdí tak často,
a většinou se potřebují ještě na něco zeptat, takže by tam stejně museli přijít.

Problémem může být určitá složitost především při zahájení využívání tohoto způsobu zasílání dat. Kromě zřízení si elektronického podpisu, což obnáší minimálně jednu osobní návštěvu akreditovaného poskytovatele certifikačních služeb, je nutná i instalace programu

využívaného finančním úřadem. Pro méně zdatné uživatele počítačů to může být překážka, kterou nemá potřebu nijak zdolávat. Takový uživatel může také namítat, že když stávající způsob funguje, proč by ho měl měnit. V neposlední řadě tato aktivita vyžaduje jak počáteční, tak i průběžné finanční náklady.

Následující názor na tuto problematiku jen dokresluje současný stav:

"Elektronické podání je stále složité, hlavně první instalace. Chce to zjednodušit," říká náměstek ministra financí přes daně Peter Chrenko s tím, že jej chce také sám vyzkoušet.

Nově by podle něj mělo elektronické přiznání fungovat tak, že by si člověk nestahoval celý systém do svého počítače, ale podával by přiznání přímo na webu daňové správy. Tento způsob budou úředníci testovat už letos na dani z příjmu firem a dani z přidané hodnoty. Pro zaměstnance podávající přiznání by mohl začít fungovat příští rok. [17]

6.3.1 Jak pracovat s aplikací Elektronické podání pro daňovou správu

Když jsem se pokusila zjistit, proč je zájem o tento způsob podání tak málo využívaný, seznámila jsem se nejprve s podmínkami, které musím před samotným zasláním dokumentů splnit. Na stránkách Ministerstva financí je tato problematika velmi srozumitelně popsána a vede uživatele krok za krokem celým procesem. [8]

Ve stručnosti uvedu postup při práci s tímto systémem a vlastní zkušenosti a názory:

- v první řadě je nutné ověřit si, zda počítač, který použijeme pro práci s touto aplikací, odpovídá části Systémové požadavky – kontrola nastavení počítače

Při ověřování si nastavení mého počítače se ukázalo, že čtyři požadavky na provozování aplikace Elektronické podání (EPO) z devíti hlásí chybu. Pokud bych chtěla konfiguraci upravit, mohla bych postupovat podle instrukcí uvedených pod jednotlivými požadavky. Když jsem se tedy pokusila pokračovat podle bodů průvodce, dostala jsem se k, mně nesrozumitelným, odborným informacím a k mnoha dalším odkazům, které se týkají instalací a úprav programů. Obávám se, že už v tuto chvíli bych potřebovala asistenci odborníka, aby se vypořádal s tímto problémem.

- dále se máme pozorně seznámit s částí Informace - Licenční podmínky

Tady jsem se dočetla, že poskytovatel nenese odpovědnost za zvláštní, náhodné, nepřímé nebo vedlejší škody, ať jsou jakékoli (včetně a bez omezení, škody ze ztrát zisku z podnikání, z přerušení podnikání, ze ztrát podnikatelských informací nebo jakékoli další zvláštní ztráty) způsobené užíváním nebo nemožností užívat toto aplikační programové vybavení (APV) nebo na základě poskytnutí nebo neposkytnutí služeb odborné pomoci, i když byl provozovatel upozorněn na možnost vzniku takových škod. Ještě nejméně ve dvou dalších bodech byla zmínka o tom, že poskytovatel nenese odpovědnost. Podle mého názoru by ale posouzení jednotlivých případů, které by se vztahovaly ke škodám způsobeným používáním daného programu nebo poskytováním služeb odborné pomoci, mělo být otázkou pro právníky.

- následně se máme seznámit s aplikací EPO

Tato část je velmi dobře a detailně zpracovaná, obohacená i o grafické znázornění. Vede uživatele krok za krokem při vyplňování formuláře a nalezneme zde i další odkazy a nápovědu. Je zde uvedena i podrobná dokumentace k elektronickému podání, kde lze nalézt velké množství informací.

- pokud souhlasíme s licenčními podmínkami, můžeme pokračovat

Zde si je možné vyplnit vybraný formulář, načíst soubor s podáním nebo potvrzením, ověřit si stav učiněného podání, zobrazit si podrobnější informace k podání písemnosti a další.

Kromě toho se zde můžeme seznámit s důležitými informacemi pro uživatele Daňového portálu jako jsou novinky, tiskové zprávy, upozornění, informace pro uživatele aplikace EPO a další.

Považuji možnost využívání elektronického podpisu a vůbec elektronické komunikace s finančním úřadem za přínosné, ale i když na portále můžeme nalézt podrobné informace, je cesta k zahájení využívání tohoto způsobu stále ještě komplikovaná a zdlouhavá.

To by mohlo vysvětlovat dosud ne příliš velký zájem organizací o jeho zprovoznění.

Vzájemnou elektronickou komunikaci s využitím elektronického podpisu si pochvalují především pracovnice úřadů při přeposílání dat (například pracovnice z pracoviště státní sociální podpory, které zasílají data na FÚ a opačně). Považují ji za rychlou a pohodlnou.

6.4 Pracoviště státní sociální podpory v Otrokovicích

Tato pobočka patří pod Úřad práce ve Zlíně, kde je i hlavní centrála. Přesto zde mají dvě pracovnice zřízený elektronický podpis a mohou tak vzájemně komunikovat jak s centrálou, tak s jinými úřady. Zkušenosti s tímto způsobem mají dobrý.

Ze strany občanů však žádný zájem nezaznamenaly nebo jen výjimečně. V případě, že by se chtěl někdo informovat na možnost využívání elektronické komunikace s tímto úřadem, odkáže ho pracovnice na hlavní centrálu ve Zlíně, kde mu budou poskytnuty bližší informace. Pokud se zájemce rozhodne zasílat dokumenty elektronicky s využitím elektronického podpisu, tak aby nemusel navštěvovat příslušný úřad osobně, bude tyto dokumenty zasílat na podatelnu ve Zlíně a ta je pak přeposílá jednotlivým úředníkům na pobočky.

6.5 Česká správa sociálního zabezpečení (ČSSZ)

I když se pobočka ČSSZ přímo na území Otrokovic nenachází, považuji ji z hlediska této bakalářské práce za tak důležitou, že se o možnostech elektronické komunikace s ní zmíním. Česká správa sociálního zabezpečení umožňuje přijímat tato elektronická podání: Evidenční listy důchodového pojištění (ELDP), přihlášky a odhlášky zaměstnanců k nemocenskému pojištění (P/O) a Přehled o příjmech a výdajích osob samostatně výdělečně činných (Přehled OSVČ). Podání se děje prostřednictvím celosvětové síťě Internet přes Portál veřejné správy (PVS) nebo na paměťovém médiu. Pro elektronickou komunikaci je nutné registrovat pověřeného pracovníka do databáze registrovaných pracovníků ČSSZ. Dříve ČSSZ vydávala podpisové klíče, ale jejich vydávání bylo již ukončeno. Nyní preferuje podpis kvalifikovaným certifikátem. Pokud chceme zasílat dokumenty elektronicky, je nutné používat programy, které komunikaci s ČSSZ umožní. Podrobnosti lze získat na webových stránkách ČSSZ.

V případě, že se zájemce z Otrokovic rozhodne využívat tohoto způsobu komunikace, musí navštívit pobočku ve Zlíně, protože v Otrokovicích se žádná nenachází.

6.6 Úřad práce v Otrokovicích

Toto pracoviště je pobočkou Úřadu práce ve Zlíně. Způsob komunikace navzájem mezi úřady, i způsob komunikace s občany a firmami, je obdobný jako u pracoviště státní sociální podpory. V případě, že zájemce využívá elektronické zasílání dokumentů, zasílá je na

centrální adresu elektronické podatelny Ministerstva práce a sociálních věcí a odtud je následně přeposlána k vyřízení jednotlivým pracovištím. V našem případě na pobočku v Otrokovicích.

6.6.1 Podmínky přijetí elektronického podání na úřadech práce

Portál Ministerstva práce a sociálních věcí poskytuje na svých stránkách podmínky, za kterých lze uskutečňovat elektronické podání. Jsou zde uvedeny formáty, ve kterých lze zasílat podání a podmínka, že se zasílá jako příloha. Dále je zde uvedena adresa elektronické podatelny. Důležitá je informace, že naše podání musí být elektronicky podepsáno kvalifikovaným certifikátem jednoho z akreditovaných poskytovatelů certifikačních služeb.

V elektronické formě lze v současné době doručovat následující podání:

- podání ve správním řízení
- plnění oznamovacích povinností daných pracovněprávními předpisy
- běžná korespondence s úřadem práce
- žádost o poskytnutí informací podle zákona č. 106/1999 Sb., o poskytování informací, v platném znění
- stížnosti a podněty týkající se činnosti zaměstnanců úřadu práce a zaměstnavatelů

V případě, že zasíláme zprávu nebo dokument bez elektronického podpisu můžeme využít přímo e-mailovou adresu příslušného úředníka. Jejich seznam nalezneme na stránkách úřadu práce.

Na tomto portálu se nachází i mnoho dalších odkazů a informací, jsou zde formuláře, kontakty a další.

Využívání elektronického podpisu v případě úřadu práce a pracovišť státní sociální podpory ze strany občanů je velmi nízké a nemyslím si, že by se zájem v budoucnu příliš rychle zvyšoval. Tato skutečnost je jistě ovlivněna i oblastmi, které byly zatím elektronickému způsobu podání zpřístupněny. S rozšiřující se nabídkou se dá předpokládat i zvyšování zájmu. Přesto očekávám, že se zvýší především ze strany zájemců, kteří již mají zřízen

elektronický podpis a využívají této služby i u jiných úřadů. Stále zůstává problém s technickou a softwarovou stránkou, protože je pro velkou část uživatelů příliš nesrozumitelná a může je od využívání těchto možností odrazovat.

7 ZÁJEM FIREM O ELEKTRONICKÝ PODPIS

Abych zjistila zájem firem z Otrokovic o využívání elektronického podpisu zvolila jsem několik způsobů sběru dat. Osobní návštěvy, telefonické dotazy a e-mailový dotazník. Pokud bych měla zhodnotit zkušenosti z jednotlivých metod, byly osobní návštěvy firem nejpřínosnější, avšak časově náročné. Telefonické dotazy jsem vyhodnotila jako rychlou a pohodlnou metodu, bohužel je nákladná. Jako nejméně vhodné se ukázalo rozesílání e-mailových dotazníků. I když bylo tímto způsobem možné obeslat velké množství firem, výsledek byl neuspokojivý. Ochota pracovníků firem odpovědět na e-mail, který pro ně není přínosem, je malá.

Ačkoli jsem věřila, že budu moci provést statistické vyhodnocení výsledků a zpracovat ho do tabulek a grafů, zjistila jsem, že téměř není co vyhodnocovat.

Ze 42 firem, které mi byly ochotné poskytnout informace, ani jedna elektronický podpis zatím nevyužívá.

V 6 firmách připustili, že o zavedení této formy komunikace s orgány veřejné správy uvažují, ale zatím neměli čas se touto otázkou zabývat.

V 8 malých firmách dokonce o existenci elektronického podpisu ani nevěděli.

Odpovědi na dotaz „Proč elektronickou komunikaci nevyužívají?“ mohu rozdělit do několika skupin:

- ve firmě o existenci elektronického podpisu neví a ani je to nezajímá

- o existenci e-podpisu ví, ale zájem ho využívat nemají, protože jim stávající způsob vyhovuje

- považují zřízení e-podpisu a elektronické propojení se s různými úřady zatím za příliš komplikované, nejednotné a celý proces za časově náročný. Nemají ve firmě nikoho, kdo by se této oblasti mohl věnovat

- zvláště některé menší firmy se vyjádřily tak, že nechtějí do této oblasti investovat

- v několika firmách připustili, že se ještě neseznámili s podrobnostmi týkajícími se elektronického podpisu, protože řeší důležitější záležitosti

Názory se sice částečně lišily, ale pokud bych je shrnula, neviděla jsem o problematiku elektronické komunikace s orgány veřejné správy příliš velký zájem a většinou šlo o hledání důvodů, proč se o tento způsob komunikace nezajímají.

8 SHRNUTÍ VÝSLEDKŮ PROVEDENÉ ANALÝZY

Provedená analýza přinesla, co se týká využívání elektronického podpisu, nečekeně nepříznivé výsledky. Zdá se, že i když je tento způsob komunikace na trhu již několik let, rozsah jeho využívání je, alespoň podle výsledků mého průzkumu, velmi malý.

Důvodem, proč jsem v Otrokovicích nenarazila na žádnou firmu, která by e-podpis využívala, může být i fakt, že se většinou jednalo o firmy s menším počtem zaměstnanců.

Jinak se dá předpokládat, že relativně malé rozšíření e-podpisu má dva hlavní důvody: stále nedostatečná propagace e-podpisu a informací o možnostech jeho využití ze strany úřadů, které nejsou ještě všude plně připraveny na čistě elektronickou agendu, a pak možná i cena, která odradí řadu poučených zájemců. Zaplatit například 752 korun za roční podpis si asi mnoho uživatelů rozmyslí a raději si zajde na poštu s doporučenou obálkou nebo na úřad osobně, neboť případná časová úspora pro ně není tak hmatatelná. I když v současné době poskytuje Česká pošta s. p. tuto službu za necelých 200 korun a tak by cena již nemusela být takovou překážkou.

Další nevýhodou je určitá nejednotnost. Při komunikaci s většinou úřadů je, kromě úpravy konfigurace našeho počítače, nutná také instalace programů, které tento způsob komunikace umožní. Přičemž co úřad, to jiné požadavky.

Z některých ohlasů uživatelů e-podpisu, které jsem si vyhledala na internetových stránkách, vyplývá, že se setkávají například s odmítnutím svého e-podpisu a pak jsou nuceni vyhledávat příčiny tohoto stavu, což samozřejmě kladnému hodnocení nijak nepřispívá.

I celková nedůvěra v tento způsob zasílání dokumentů může hrát svoji roli.

V neposlední řadě bych nezájem o využívání e-podpisu viděla také v neochotě měnit fungující způsob komunikace s orgány veřejné správy, kterým je buď osobní návštěva nebo zaslání dokumentů poštou..

Celou situaci dokresluje i následující statistika: je to statistika, která sleduje zájem veřejných subjektů, firem a fyzických osob o certifikáty, které jsou jedním z hlavních nástrojů pro podepisování, identifikaci a autentizaci osob v prostředí internetu či šifrování. Poslední statistické údaje uvedené na webových stránkách Ministerstva vnitra jsou sice jen po první čtvrtletí roku 2007, přesto nabízí alespoň orientačně rozsah využívání tohoto způsobu ko-

munikace v ČR. K 30. dubnu 2007 bylo v ČR celkem 43 088 platných kvalifikovaných certifikátů. [13]

Toto množství považuji za velmi nízké.

9 NÁVRH DOPORUČENÍ

V současné době vykazuje využívání elektronického podpisu určitou stagnaci nebo jen pozvolný nárůst zájemců. Ten, kdo si pořídit elektronický podpis chtěl, už to udělal a dalších zájemců příliš nepřibývá nebo vyčkávají.

Když jsem na úřadech řešila otázku, jak zlepšit povědomí společností o elektronickém podpisu a zvýšit jejich zájem o jeho využívání, většinou jsme se shodli na tom, že pouhé přesvědčování ze strany úředníků nestačí. Určitou cestou by bylo zpoplatnění osobně předávaných dokumentů, které se musí na úřadech převádět do elektronické podoby. Podobně řešily situaci banky, které zvýšily poplatky za služby poskytované na přepážkách a odkazovaly klienty na levnější možnost komunikace přes elektronické služby. Tento způsob opravdu osobní návštěvy přepážek bank snížil.

Jiným způsobem, který by mohl pomoci s větším rozšířením využívání elektronického podpisu, by bylo sjednocení požadavků na počítačové a programové vybavení uživatelů, případně využívání pouze jednoho portálu, na kterém by bylo možné vyplňovat různé formuláře a následně je přímo z tohoto portálu odesílat podepsané elektronickým podpisem. Značně by se tak snížila celková nepřehlednost.

Další příčinu můžeme spatřovat v omezeném počtu úředních úkonů, které lze tímto způsobem vyřídit. Většina zákonů totiž stále vyžaduje identifikaci formou originálního podpisu oprávněných osob, vyplnění originálních tiskopisů či použití úředního razítka, což elektronický podpis neumožňuje. Proto, aby se zájem o používání tohoto podpisu zvýšil, bude nutné umožnit vyplňovat a odesílat větší množství typů formulářů jednotlivých úřadů.

Zavedení možnosti komunikovat s orgány veřejné správy bylo jistě velmi nákladné a tak by byla škoda, aby zůstalo využíváno jen úzkým okruhem zájemců.

ZÁVĚR

V bakalářské práci, která se věnovala možnosti využívání elektronického podpisu při komunikaci s orgány veřejné správy, jsem se snažil podat ucelenou informaci o elektronickém podpisu. Objasnila jsem principy, na nichž je elektronický podpis založen a vysvětlila jsem pojmy, které s touto problematikou souvisí, jako jsou asymetrická kryptografie, hash funkce, elektronická značka nebo e-podatelna. Pozornost jsem věnovala i legislativnímu zakotvení elektronického podpisu jak v České republice, tak v některých státech Evropské unie.

Dále jsem zjistila současný stav využívání tohoto podpisu na území města Otrokovice, výsledky jsem zhodnotila a pokusila se navrhnout způsob, jak zvýšit zájem o jeho využívání.

Pokud se vrátím k důvodu, který mě vedl ke zpracování tohoto tématu a měla bych se rozhodnout, zda doporučit používání elektronického podpisu v naší firmě, musím se přiznat, že po prostudování dané problematiky, bych si jeho významným přínosem nebyla příliš jistá. Ale na zkoušku bych možná požádala o možnost komunikovat alespoň s jednou institucí, například s ČSSZ, a po vyhodnocení zkušeností bychom se rozhodli na dalším postupu.

Na závěr bych vyslovila přesvědčení, že i když výsledky analýzy využívání elektronického podpisu v praxi v mé bakalářské práci nevyzněly příliš pozitivně, věřím, že elektronická komunikace včetně využívání tohoto podpisu má před sebou slibnou budoucnost. Vývoj jde nezadržitelně vpřed a lze očekávat další zdokonalování elektronického podpisu, ale zároveň i zjednodušování používání elektronické komunikace, které umožní její využívání širší veřejnosti.

SEZNAM POUŽITÉ LITERATURY

Monografie:

[1] BOSÁKOVÁ, Dagmar. *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.

[2] JAŠEK, Roman. *Informační a datová bezpečnost.* 1. vyd. Zlín: Univerzita Tomáše Bati, 2006. 141 s. ISBN 80-7318-456-7.

[3] JAŠEK, Roman. *Ochrana znalostí a dat v podnikových systémech.* 1. vyd. Zlín: Univerzita Tomáše Bati, 2002. 115 s. ISBN 80-7318-095-2.

[4] ROSMAN, Pavel, et al. *Informatika pro ekonomy.* 2. upr. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006. 233 s. ISBN 80-7318-430-3.

Internetové zdroje:

[5] *Archiv stránek bývalého Ministerstva informatiky* [online]. [cit. 2008-02-21]. Dostupné na WWW: <http://www.mvcr.cz/micr/scripts/detail.php_id_1799.html>.

[6] *Certification authority: Využití časových razítek.* [online]. [cit. 2008-04-15].

Dostupné na WWW:
<http://www.ica.cz/home_cs/?acc=casova_razitka_a_casove_autority>.

[7] *Certifikační politika I. CA : pro vydávání komerčních certifikátů* [online]. c2002 [cit. 2008-04-01]. Verze 1.04.

Dostupné na WWW: <http://www.ica.cz/dokumenty/cp_ica_104.pdf>.

[8] *Česká daňová správa* [online]. [cit. 2008-04-03]. Dostupné na WWW:

<https://adisdpr.mfcr.cz/adistc/adis/idpr_pub/dpr/uvod.faces>.

[9] *Česká pošta s. p. Produkty.* [online] [cit. 2008-04-02]. Dostupné na WWW:

< http://www.cpost.cz/jetspeed/?js_language=cz >.

[10] *EIdentity. Popis poskytovaných služeb.* [online]. [cit. 2008-04-09].

Dostupné na WWW: <https://www.eidentity.cz/ServicesDescription.html>.

[11] HOBZA, Jan. *Elektronický podpis: legislativa a jeho zavádění v členských státech Evropské unie. Veřejná správa: týdeník vlády České republiky.* [online]. [cit. 2008-04-09].

Dostupné na WWW: <http://www.mvcr.cz/casopisy/s/2002/0012/pril1.html>.

[12] *Hutnická zaměstnanecká pojišťovna.* [online]. [cit. 2008-04-25].

Dostupné na WWW: <http://www.hzp.cz/main/clanek.php?id=1133>.

[13] *Ministerstvo vnitra: Elektronický podpis.* [online]. [cit. 2008-04-15].

Dostupné na WWW:
<http://www.mvcr.cz/micr/images/statistiky/epodpis2007.pdf>.

[14] *Ministerstvo vnitra: Vyhláška č. 378/2006 Sb.* [online]. [cit. 2008-04-15].

Dostupné na WWW: <http://www.micr.cz/micr/scripts/detail.php_id_3630.html>.

[15] *Obecné informace : O společnosti* [online]. c2000 [cit. 2008-04-01]. Dostupné na WWW: <http://www.ica.cz/home_cs/?acc=o_spolecnosti>.

[16] *Otrokovice Informační portál* [online]. [cit. 2008-04-03]. Dostupné na WWW:

<http://www.otrokovice.cz/newwebotr/InformaceUrad/epodatelna.aspx?id=ep>.

[17] PATOČKOVÁ, Martina. *iDnes: Daně se budou platit bez papíru, ale s větší kontrolou.* [online]. [cit. 2008-04-20].

Dostupné na WWW: <http://ekonomika.idnes.cz/dane-se-budou-platit-bez-papiru-ale-s-vetsi-kontrolou-p0k-/ekonomika.asp?c=A080416_210412_ekonomika_dp>.

[18] *PCTuning: Moderní metody šifrování.* [online]. [cit. 2008-04-03].

Dostupné na WWW:
<http://pctuning.tyden.cz/index.php?option=com_content&task=view&id=4711&Itemid=41>.

[19] *Podatelna.info: Elektronická podatelna.* [online]. [cit. 2008-04-10]. Dostupné na WWW: <http://podatelna.info/index.php3?s1=popis&s2=podani&lng=cz>.

[20] *Portál veřejné správy: Elektronický podpis.* [online]. [cit. 2008-04-03].

Dostupné na WWW: <http://portal.gov.cz/wps/portal/_s.155/696/_s.155/708?uzel=7&POSTUP_ID=574>.

[21] *Portál zdravotních pojišťoven.* [online]. [cit. 2008-04-25]. Dostupné na WWW: <http://www.portalzp.cz/zpravodaj.html>.

[22] *SMĚRNICE 1999/93/EC EVROPSKÉHO PARLAMENTU A RADY: o zásadách Společenství pro elektronické podpisy.* [online]. [cit. 2008-04-10]. Dostupné na WWW: <http://www.businessinfo.cz/files/file2122.pdf>.

[23] *Všeobecná zdravotní pojišťovna.* [online]. [cit. 2008-04-25]. Dostupné na WWW: <http://www.vzp.cz/cms/internet/cz/Vseobecne/Portal/>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

3DES	Typ algoritmu (Triple – DES).
a.s.	Akciová společnost.
ACAeID	Akreditovaná certifikační autorita eIdentity a.s.
APV	Aplikační programové vybavení.
CA	Certifikační autorita.
CCA	Komerční certifikační autorita.
CRL	Seznam zneplatněných certifikátů.
ČR	Česká republika.
ČSOB	Československá obchodní banka.
ČSSZ	Česká správa sociálního zabezpečení.
DES	Typ algoritmu.
DIČ	Daňové identifikační číslo.
EESSI	Evropská iniciativa pro normalizaci elektronických podpisů.
ELDP	Evidenční list důchodového pojištění.
EPO	Elektronické podání.
ETSI	Evropský ústav pro telekomunikační normy.
EU	Evropská unie.
FAQ	Často pokládané otázky.
FÚ	Finanční úřad.
HTML	Jazyk, který slouží k tvorbě webových stránek.
HZP	Hutnická zaměstnanecká pojišťovna.
I.CA	Registrační autorita.
IČO	Identifikační číslo organizace.
IDEA	Typ algoritmu.

MIČR	Ministerstvo informatiky České republiky.
OP	Občanský průkaz.
OSVČ	Osoba samostatně výdělečně činná.
P/O	Přihlášky a odhlášky zaměstnanců k nemocenskému pojištění.
PID	Identifikační číslo podání.
PVS	Portál veřejné správy.
QCA	Kvalifikovaná certifikační autorita.
RSA	Typ algoritmu.
SMS	Krátká textová zpráva.
TSA	Autorita časových razítek.
VCA	Veřejná certifikační autorita.
VZP	Všeobecná zdravotní pojišťovna.
ZP	Zdravotní pojišťovna.

SEZNAM OBRÁZKŮ