

Univerzita Karlova v Praze

Filozofická fakulta

Ústav informačních studií a knihovnictví

Studijní program: informační studia a knihovnictví

Studijní obor: informační studia a knihovnictví

Bakalářská práce

Čeněk Kudrna

**Využití elektronického podpisu pro zajištění komunikace občana s
veřejnou správou**

**Utilization of electronic signature for providing communication
between citizen and public administration**

Praha 2010

Vedoucí práce: PhDr. Hana Slámová, Ph.D.

Oponent bakalářské práce:

Datum obhajoby:

Hodnocení:

zadání

Prohlášení:

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

V Praze, dne 8.7. 2010

.....
podpis studenta

Identifikační záznam

KUDRNA, Čeněk. *Využití elektronického podpisu pro zajištění komunikace občana s veřejnou správou = Utilization of electronic signature for providing communication between citizen and public administration* Praha, 2010-07-19. 72 s, . příl. Bakalářská práce (Bc.). Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví. Vedoucí bakalářské práce Hana Slámová.

Abstrakt (česky)

Tato bakalářská práce se zaměřuje na využití elektronického podpisu pro zajištění komunikace občana s veřejnou správou v České republice. Práce je rozdělena do devíti kapitol. Úvodní část je věnována společenským podmínkám, které ovlivňovaly vývoj celého systému elektronické veřejné správy. Práce také charakterizuje důležité termíny problematiky elektronického podpisu. Práce se také věnuje bezpečnosti elektronické komunikace a jejích problémům. V práci jsou shrnuty základní legislativní dokumenty zaměřené na eGovernment a elektronický podpis. Další část popisuje postup pro získání certifikátů potřebných k vytvoření elektronického podpisu. V případové studii o zřízení kvalifikovaného certifikátu jsou pak tyto postupy ověřeny. Práce také obsahuje statistiky zaměřené na využívání elektronických služeb ke komunikaci se státní správou.

Abstrakt (anglicky)

This bachelor thesis is focused on utilization electronic signature for providing communication between citizen and public administration in Czech Republic. The thesis is divided to nine chapters. The introduction section is devoted to social conditions that influenced the development of system electronic public administration. The thesis also characterizes important terminology of the electronic signature's issue. The paper also deals with the question of security of electronic communication and its other problems. Following part summarizes basic legislative documents aimed at eGovernment and electronic signature. Next part describes the procedure of obtaining certificates needed for creating your own electronic signature. In the case study based on the establishment of qualified certificate then verified these procedures. The paper also includes statistics focused on the usage of electronic services for communication with the government.

Klíčová slova (česky)

veřejná správa, elektronický podpis, eGovernment, kryptografie, Ministerstvo vnitra České republiky, elektronické podání, Portál veřejné správy České republiky, informační systém, eGON, certifikáty, bezpečnostní politika

Klíčová slova (anglicky)

Public administration, electronic signature, eGovernment, Cryptography, Ministry of the Interior, of the Czech Republic, electronic submission, computerization, Public administration portal of the Czech Republic, Information System, eGon, Certificates, Security policy

Obsah

Předmluva	9
1. Úvod.....	11
2. Elektronický podpis jako nástroj eGovernmentu.....	12
2.1 Vývoj české elektronické státní správy	12
2.2 Hlavní projekty českého eGovernmentu.....	14
2.2.1 Portál veřejné správy	14
2.2.2 eGon.....	16
2.3 Současný stav eGovernmentu.....	17
2.4 Shrnutí.....	18
3. Vymezení základních pojmů	19
4. Elektronická komunikace a její bezpečnost.....	26
4.1 Ochrana elektronické komunikace.....	26
4.2 Šifrování.....	27
4.3 Typy úrovně ochrany zpráv pomocí šifrování	30
4.4 Právní ochrana	32
4.5 Užití v praxi	33
4.6 Problémy bezpečnosti elektronické komunikace.....	34
5. Právní rámec pro využití elektronického podpisu v elektronických dokumentech	36
5.1 Komise UNCITRAL.....	36
5.2 Směrnice 1999/93/ES	37
5.3 Zákon 227/2000 Sb., o elektronickém podpisu	37
5.3.1 Jednotlivá témata zákona č. 227/2000 Sb.....	38
5.4 Vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb	41
5.5 Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů	42
5.6 Shrnutí.....	42
6. Možnosti zřízení elektronického podpisu, jeho použitelnost, jeho výhody i nevýhody.....	45
6.1 Možnosti zřízení	45
6.2 Poupitelnost zaručeného elektronického podpisu	47
6.3 Výhody a nevýhody elektronického podpisu.....	50
7. Získání kvalifikovaného certifikátu na pobočce České pošty	51

7.1 Získání kvalifikovaného certifikátu pro účely komunikace s veřejnou správou	51
7.2 Hodnocení uživatele	54
8. Průzkum na téma využití elektronického podpisu v praxi.....	55
9. Závěr	58
Seznam použité literatury	60
Seznam obrázků.....	64
Seznam tabulek	64
Seznam grafů	64

Předmluva

Tématem bakalářské práce je využití elektronického podpisu pro zajištění komunikace občana s veřejnou správou. Práce je zaměřena na prostředí České republiky. Důvodem pro výběr tohoto tématu je autorův zájem o nové technologie, moderní pojetí státní správy a osobní zaujetí o státní správu, kde by autor práce chtěl najít své budoucí uplatnění.

Záměrem práce je prezentovat technologii a procesy spojené s elektronickým podepisováním dokumentů při komunikaci s úřady veřejné správy. Práce by měla popsat všechny aspekty zaměřené na tento nový druh komunikace s úřady.

První kapitola je věnována společenským podmínkám, které vedly k zavedení elektronického podpisu do systému veřejné správy. Protože eGovernment je úzce spjat s elektronickým podpisem, je v této úvodní kapitole shrnut vývoj celého systému eGovernmentu v České republice.

Druhá kapitola obsahuje základní pojmy problematiky elektronického podpisu. Vyjmenované termíny jsou charakterizovány definicemi z legislativních dokumentů nebo odborných publikací.

O bezpečnosti elektronické komunikace pojednává třetí kapitola. Popisuje základní principy bezpečnosti komunikace a metody ochrany komunikace prostřednictvím elektronického podepisování. Hlavní část kapitoly se věnuje šifrování komunikace, tedy kryptografii. V další pasáži je uvedena právní ochrana eGovernmentu. Dále jsou v kapitole shrnuty problémy spjaté s využíváním elektronického podpisu.

V páté kapitole se autor práce zaměřuje na právní rámec elektronického podpisu. Jsou zde uvedeny nejdůležitější legislativní dokumenty, které vymezují celou problematiku. V úvodu jsou uvedeny evropské dokumenty, na jejichž základě vznikají zákony o elektronickém podpisu v řadě evropských zemí. Hlavní část kapitoly se věnuje zákonu č. 227/2000 Sb., o elektronickém podpisu. Tento zákon je pro tuto problematiku nejdůležitější. V závěru kapitoly najdeme názory odborníků na otázku legislativy elektronického podpisu.

V další kapitole se autor zaměří na možnosti zřízení elektronického podpisu v České republice. Popisuje obecné postupy pro získání certifikátu u kvalifikovaného poskytovatele certifikačních služeb. Dále se zabývá možnostmi užití elektronického podpisu ve státní správě. V této kapitole jsou shrnuty problémy celé technologie elektronického podpisu.

Sedmá kapitola je pojata jako případová studie věnována celému procesu získání kvalifikovaného certifikátu na pobočce České pošty. Autor práce pak v podkapitole uvádí své osobní ohodnocení této služby.

V části o průzkumu využívání elektronického podpisu nemohly být uvedeny všechny aktuální statistiky, protože dané společnosti neposkytují tyto informace z interních důvodů. Autor práce kontaktoval příslušné osoby, avšak nedošlo ke kladnému vyřízení žádosti o příslušné údaje. Kapitola tedy shrnuje rozšíření využívání počítačů s připojením k síti internet a statistické údaje o využívání elektronických služeb v rámci veřejné správy.

Jako hlavní zdroje informací byly využity převážně oficiální internetové zdroje Ministerstva vnitra České republiky nebo Portálu veřejné správy.

Práce byla zpracována dle normy ISO 690 a ISO 690-2. Citace jsou zapsány v hranatých závorkách pomocí prvního údaje záznam, data vydání a v případě číslovaných dokumentů jsou uvedeny čísla stran. Součástí práce jsou jednotlivé obrázky, tabulky a grafy převzaté z oficiálních stránek nebo vytvořené autorem práce.

Na závěr velmi děkuji své vedoucí práce PhDr. Haně Slámové Ph.D. za hodnotné připomínky a jejímu přístupu k sepsání tohoto elaborátu. Velké poděkování náleží i mé rodině, která mi umožnila tuto problematiku zpracovat a také mi svou trpělivostí a přístupem vytvořila vhodné podmínky pro zhotovení bakalářské práce.

1. Úvod

Sametová revoluce v listopadu 1989 přinesla mnoho změn, které zde není nutné uvádět. S demokratizací celého státu se samozřejmě demokratizoval i státní aparát veřejné správy. Změna ideového přístupu vedla k myšlenkám, jak nejlépe zajistit komunikaci mezi občanem a úřady. Právě v této době se došlo k názoru, že je třeba styk občana se státními institucemi zjednodušit, zrychlit a zefektivnit. Tak vznikla myšlenka sjednotit všechny informační systémy státní správy v jeden kvalitní centrální systém. To však nebylo jednoduché, protože zde chyběly zkušenosti, technologické zázemí, finanční a legislativní podpora.

Do 90. let 20. století byly systémy orgánů veřejné správy vesměs zpracovány ve formě papírových kartoték, matrik, evidencí a jiných klasických forem. Občan se tedy vždy musel dostavit na úřad osobně, pokud chtěl využít jeho služby. Protože neexistoval centrální úřad, kde by si občan mohl zařídit všechny potřeby, bylo třeba navštěvovat několik různých institucí. Vývoj výpočetní techniky ovšem přinesl nové možnosti. Větší dostupnost hardwarového i softwarového vybavení přineslo pokrok nejen v podobě digitalizace všech evidencí a kartoték, ale také v možnosti vzdáleného přístupu k datům uloženým ve vzdálené databázi.

Občan se tedy musel osobně dostavit na příslušný úřad a všechny dokumenty opatřit svým vlastnoručním podpisem. Tím byla stvrzena platnost těchto dokumentů. Pokrok v elektronické komunikaci však přinesl možnost druhou. Pro občana rychlejší a pro úřady ekonomičtější prostředek komunikace, elektronický podpis. Tento termín je třeba pro další pochopení vymezit hned na začátku této práce.

Elektronický podpis lze charakterizovat jako soubor dat jasně identifikující autora textu a stvrzující neporušenost elektronického dokumentu. V oblasti veřejné správy se jedná o druhý způsob (vedle vlastnoručního podpisu), jak stvrdit platnost právního úkonu. Dalším definicím elektronického podpisu je věnována kapitola 3.

S příchodem elektronické komunikace však nastal problém, jak zabezpečit autorství a pravost dokumentu. Při klasickém osobním styku byly tyto otázky vyřešené, ale při vzdálené komunikaci bylo třeba vytvořit zvláštní zákony a technologii, které by tyto dva způsoby komunikace ustanovily na stejnou úroveň. Právě problematikou pravosti elektronických dokumentů se zabývá tato práce.

2. Elektronický podpis jako nástroj eGovernmentu

Elektronický podpis nefunguje sám o sobě. Je to „pouze“ technologie, díky které lze opatřit elektronický dokument identifikací člověka. V prostředí státní správy je tento podpis základním nástrojem pro vzdálenou elektronickou komunikaci mezi občanem a orgány státní správy. Tento druh správy označujeme jako elektronickou vládu, tzv. e-vládu. Na celém světě se však užívá termínu eGovernment¹.

Cílem eGovernmentu je vytvořit jednotný informační systém² veřejné správy, který podstatně sníží administrativní zatížení a finanční náročnost státní správy. Systém by měl obsahovat a následně zprostředkovávat všechny údaje a informace, které státní správa může nabídnout občanům. Celý projekt přispěje k rychlejší a efektivnější komunikaci se státními institucemi. Jako každý správně fungující systém musí mít svá pravidla a jasně dané postupy, aby se zamezilo případnému narušení či zneužití. Pomocí elektronického podpisu je toho možné docílit. Nesmíme však opomenout legislativní zabezpečení poskytující ochranu v právní rovině.

Tato kapitola se věnuje vývojem, dnešním stavem a hlavními projekty elektronické státní správy.

2.1 Vývoj české elektronické státní správy

Celý projekt eGovernmentu byl zahájen v 90. letech 20. století, tedy s nástupem demokracie. Nadšení z nových možností vedlo k tomu, že akce byla zpočátku nekoordinovaná. Chyběly finance, technické zázemí i odborná pracovní síla. Také chyběla legislativa upravující postupy jednotlivých subjektů.

Za pokrok je považováno zřízení Ministerstva hospodářství zákonem č. 474/1992 Sb. Ministerstvu byla svěřena působnost v oblasti státního informačního systému. Avšak nedošlo k vydání zvláštního zákona, který by tuto působnost konkretizoval.

V roce 1992 vláda vznesla požadavek, aby v následujícím roce byl předložen návrh globální architektury informační soustavy České republiky. Vláda měla zájem podporovat rozvoj komplexního informačního systému. Předpokládalo se, že k realizaci projektu bude vydán zákon, který určí působnost jednoho ústředního orgánu, který bude provádět analýzu situace a navrhopvat společné principy Informačního systému veřejné správy. Principy by pak

¹ eGovernment je využívání informačních technologií veřejnými institucemi pro zajištění výměny informací s občany, soukromými organizacemi a jinými veřejnými institucemi za účelem zvyšování efektivity vnitřního fungování a poskytování rychlých, dostupných a kvalitních informačních služeb [Lidinský, 2008, s. 7].

realizovaly jednotlivé rezorty. Zde se však naskytly problémy. Tomuto úřadu nebyla stanovena působnost, proto nemohl být projekt uskutečněn. Rezorty ministerstev zřejmě nechtěly, aby jim zvnějšku bylo určováno, jak mají vytvářet a provozovat svoje informační systémy.

Vláda se budováním státního informačního systému dále zabývala až v roce 1995, kdy vyslovila souhlas s projektem Výstavby státního informačního systému České republiky s využitím komunikační sítě Ministerstva financí ostatními rezorty.

Zákonem č. 272/1996 Sb. bylo zrušeno Ministerstvo hospodářství. Tento zákon však zřídil Úřad pro státní informační systém, na který přešla působnost zaniklého ministerstva. V roce 1999 vypracoval úřad materiál „Státní informační politika – cesta k informační společnosti“ a na něj navazující „Koncepti budování informačních systémů veřejné správy“. Informační systém veřejné správy v něm byl vymezen jako komplex jednotlivých informačních systémů, které provozuje správa a samospráva, přičemž jeho jádrem měl být státní informační systém.

V roce 2000 se Úřad pro státní informační systém změnil na Úřad pro veřejné informační systémy. Úřadu byly svěřeny působnosti dle zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů.

Situace se změnila v roce 2002, kdy vláda svým programovým prohlášením dala najevo, že budování informačního systému veřejné správy by mohlo posloužit jako nástroj pro snížení nákladů. Také by to vedlo ke zvýšení komfortu vztahu občana a státu. Zákonem č. 517/2002 Sb. došlo ke zrušení Úřadu pro veřejné informační systémy a k následnému zřízení Ministerstva informatiky. Tím vznikl ústřední orgán pro správu informační a komunikační technologie, pro telekomunikaci a poštovní služby. Hlavním přínosem tohoto ministerstva bylo zahájení projektu **Elektronický podpis obcím**³ v roce 2004, které nabídlo obcím bezplatné získání certifikátů pro elektronický podpis. Po 4 letech působení bylo ministerstvo zrušeno. Problematiku elektronizace veřejné správy převzalo v roce 2007 Ministerstvo vnitra. Jako poradní orgán pro tuto problematiku funguje Rada vlády pro informační společnost.

V březnu roku 2004 vláda schválila dokument „Státní informační a telekomunikační politika e-Česko 2006“. V návaznosti na Akční plán Evropské unie eEurope 2005, byly v této oblasti stanoveny následující priority:

- zajištění dostupné a bezpečné komunikační služby,

³ Hlavní podstatou je hromadná objednávka kvalifikovaných certifikátů u dosud jediné akreditované certifikační autority (I.CA) v počtu dostačujícím pro všech 6235 obcí v ČR. Certifikáty byly vydávány pro starosty či pro obcí pověřené osoby [Peterka, 2004].

- informační vzdělanost,
- moderní veřejné služby on-line,
- dynamické prostředí pro elektronické podnikání.

Roku 2006 byla vydána Národní strategie informační bezpečnosti ČR, která byla vypracována na základě úkolu stanoveném v dokumentu Státní informační a komunikační politika e-Česko 2006 [Mates, 2006, s. 9-29].

Z výše uvedených prohlášení a zákonů si lze udělat obrázek, jaká byla snaha o zavedení elektronizace do veřejné správy. Počáteční neúspěchy můžeme přičítat nedokonalé technice, nebo nevoli orgánů vytvořit kompletní systém. Nedílnou součástí strastiplné cesty byla finanční stránka celého projektu. Jednalo se o velmi nákladný projekt, kdy se musí vybavit velké množství pracovišť a vyškolit dostatečný počet pracovníků. Vidíme však snahu na straně většiny vlád, které se na politickém poli vystřídaly v průběhu posledních 20 let, že projekt eGovernmentu, respektive elektronického podpisu, má znatelnou podporu. Česká republika sice nedosahuje takových výsledků jako jiné země, ale má značnou výhodu v podobě lepších startovacích podmínek a také možnosti čerpání zkušeností z jiných zemí, v nichž má eGovernment delší tradici.

2.2 Hlavní projekty českého eGovernmentu

Elektronizaci veřejné správy zajišťují dva hlavní projekty. Jejich úlohy a cíle jsou popsány níže.

2.2.1 Portál veřejné správy

Portál veřejné správy je vlastně elektronická brána do veřejné správy. Vznikl zákonem č. 365/2000 Sb., o informačních systémech veřejné správy. Cílem projektu je usnadnit občanům a firmám orientaci a komunikaci s úřady veřejné správy. Portál také významným způsobem přispívá ke zkvalitnění služeb poskytování garantovaných a důvěryhodných informací občanům ČR i cizincům. Účelem projektu je také zvýšení transparentnosti správního a ekonomického prostředí s cílem zvýšit důvěryhodnost a posílení autority veřejné správy. Významně se také podílí na její modernizaci prostřednictvím informačních a komunikačních technologií. Tím se naplňuje motto „Efektivní veřejná správa a přátelské služby“ [Česko, ©2010d].

Česká republika

- » [Informace o ČR](#)
- » [Prezident](#)
- » [Parlament](#)
- » [Vláda](#)
- » [Ministerstva](#)

Kraje



Evropská unie

- » [Informace o EU](#)



Občan





Podnikatel



Cizinec



Informace pro uživatele

Vážení uživatelé, v rámci zkvalitnění služeb dochází od 1.7.2010 ke změně kontaktních údajů pro podporu uživatelů Informační části Portálu. Nově se můžete obracet na telefonní číslo  **800 888 782**  (v případě nedostupnosti na  **731 119 418** ) nebo e-mailovou adresu: pvs@kshelp.cz

Detailní informace naleznete v sekci [Kontaktní údaje](#).

Novinky z veřejné správy

- 23.7.2010** [Úřad vlády ČR - Dny otevřených dveří ve vile Hany a Edvarda Benešových v Sezimově Ústí](#) - O víkendu 24. a 25.7...
- 23.7.2010** [Státní zemědělská a potravinářská inspekce - Jak je to doopravdy s novými požadavky na tzv. "éčka"](#) - V platnost vstupuje...
- 23.7.2010** [Evropská komise - "Poučení o právech" pro osoby podezřelé ze spáchání trestné činnosti](#) - Komise navrhuje předpis...
- 23.7.2010** [Ministerstvo zahraničních věcí ČR - Prohlášení MZV k vydání poradního posudku ICJ](#) - MZV ČR vítá...
- 23.7.2010** [Evropský parlament - Systémy zdravotní péče v subsaharské Africe](#) - Efektivitu evropské zahraniční pomoci...

[Další Novinky z veřejné správy >>>](#)

Povinně zveřejňované informace

- 23.7.2010** [114/1992 Sb. - Plán péče o CHKO Labské pískovce](#) - Ministerstvo životního prostředí...
- 23.7.2010** [114/1992 Sb. - Plán péče o PP Nad Vápenkou](#) - Krajský úřad Jihomoravského kraje...
- 21.7.2010** [114/1992 Sb. - Plán péče o NPP Dunaiovecké kopce](#) - Ministerstvo životního prostředí...
- 21.7.2010** [114/1992 Sb. - Plán péče o NPP Miroslavské kopce](#) - Ministerstvo životního prostředí...
- 21.7.2010** [114/1992 Sb. - Plán péče o PR Hraniční louka a PP Velká louka](#) - Správa CHKO Orlické hory...

[Další Povinně zveřejňované informace >>>](#)

Novinky na portal.gov.cz

Užitečné

- » [Obchodní věstník](#)
- » [Veřejné zakázky](#)
- » [Katalog informačních zdrojů](#)
- » [Práce](#)
- » [Náhled do katastru nemovitostí](#)
- » [Povodňové informace](#)
- » [Dopravní zpravodajství](#)
- » [Digitální vysílání](#)
- » [Databáze konzultujících organizací \(DataKO\)](#)
- » [Veřejná diskuze k vládním materiálům](#)
- » [Připravovaná legislativa](#)
- » [Hodnocení dopadů regulace \(RIA\)](#)
- » [Volná pracovní místa](#)
- » [Volby 2010](#)

Oblasti veřejné správy

- » [Právo a zákony](#)
- » [Práce a sociální věci](#)
- » [Obchod - průmysl](#)
- » [Finance](#)
- » [Vnitro](#)
- » [Obrana a bezpečnost](#)
- » [Zahraníčí](#)
- » [Doprava](#)
- » [Školství](#)
- » [Kultura](#)
- » [Životní prostředí](#)
- » [Zemědělství](#)
- » [Místní rozvoj](#)
- » [Zdraví](#)
- » [Informatika](#)

Obr. 1 Úvodní stránka Portálu veřejné správy České republiky

[Česko, ©2003-2010]

Portál je budován na základě spolupráce mezi jednotlivými ministerskými resorty. Výsledkem je katalog životních situací, jenž obsahuje návody postupů při jejich řešení. Dále se na portálu nacházejí plná znění zákonů. Občan zde také může nalézt kompletní seznam úřadů v České republice a pomocí vyhledávání získat kontaktní údaje k dané instituci. Velmi důležitou částí portálu je část elektronického podání, kde občan může pomocí elektronického podpisu komunikovat s veřejnou správou (více Kapitola 6). Pro informovanost občanů portál nabízí slovník pojmů objevujících se v celém systému veřejné správy. Úvodní strana portálu (Obr. 1) je řešena v rámci zajištění jednoduchosti a stručnosti.

2.2.2 eGon

eGon představuje komplexní projekt elektronizace veřejné správy, jehož cílem je usnadnit život občanům a zvýšit efektivitu veřejné správy pomocí důmyslného využití informačních technologií [Česko, ©2010d].

Projekt byl zahájen v roce 2006 a již v roce 2007 byl zahájen provoz první části – CzechPoint.⁴ Byly zveřejněny návrhy legislativních úprav podmiňující vlastní realizaci celého projektu. Přijetím zákona č. 300/2008 Sb., o autorizované konverzi dokumentů, byl celý projekt spuštěn. V dalším roce 2009 byl projekt rozšířen o datové schránky a Komunikační infrastrukturu veřejné správy (dále jen KIVS)⁵. Rok 2010 byl testovacím rokem základních registrů⁶.

Projekt je graficky spjat s postavičkou eGon (Obr. 2). Představuje moderní, přátelský a efektivní úřad. Jeho části lze popsat následovně:

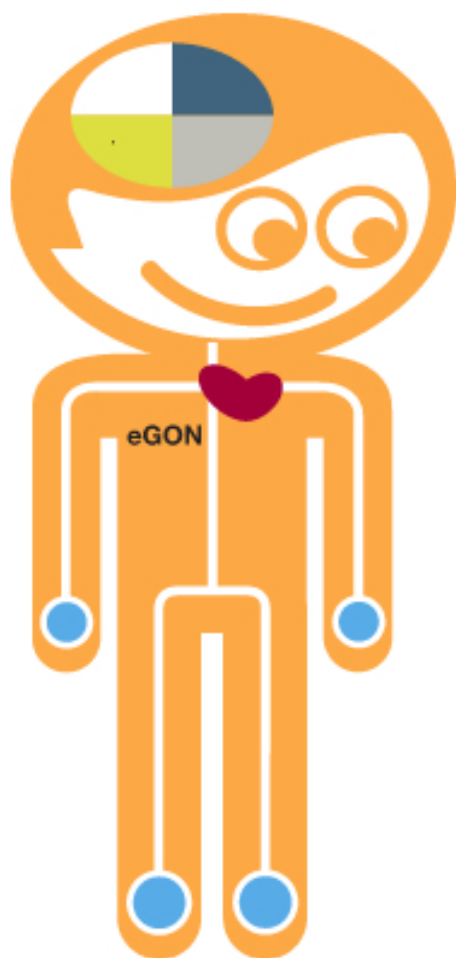
- **Prsty:** Czech POINT - soustava snadno dostupných kontaktních míst
- **Oběhová soustava:** KIVS – Komunikační infrastruktura veřejné správy, zajišťující bezpečný přenos dat
- **Srdce:** Zákon o eGovernmentu - zákon o elektronických úkonech a autorizované konverzi č.300/2008 Sb.
- **Mozek:** Základní registry veřejné správy- bezpečné a aktuální databáze dat o občanech a státních i nestátních subjektech

[Česká republika, 2008]

⁴ CzechPoint znamená Český Podací Ověřovací a Informační Národní Terminál. Jde o kontaktní místo veřejné správy, poskytující občanům ověřené údaje vedené v centrálních registrech.

⁵ KIVS představuje sjednocení různých datových linek subjektů veřejné správy do jedné datové sítě.

⁶ Jedná se o 4 registry obyvatel, práv a povinností, osob a územní identifikace, adres a nemovitostí. Základem je tzv. referenční údaj, který bude přebírán ze všech systémů základních registrů. Pokud dojde k jeho změně (např. změna adresy občana), nový údaj se promítne ve všech ostatních registrech.



Obr. 2 Postavička eGon

[Česko, ©2010d]

2.3 Současný stav eGovernmentu

Současná finanční krize může paradoxně přispět k realizaci vládní vize. Pokud se vláda rozhodne investovat velké finance do státních zakázek, aby „nastartovala“ ekonomiku, budou projekty elektronizace veřejné správy rozšiřovány a zkvalitňovány. Protože projekty v soukromém sektoru jsou pozastaveny, je na trhu dostatečná výrobní kapacita na plnění státních zakázek. Přičteme-li finanční prostředky z EU, nestojí projektům téměř nic v cestě. Vládní vize v oblasti eGovernmentu má tedy slibné vyhlídky na úspěch [Luhan, 2009, s. 16].

2.4 Shrnutí

Z výše uvedeného lze konstatovat, že se v České republice vytváří dobré podmínky pro elektronickou komunikaci se státní správou. Záleží však na počtu lidí - uživatelů, kteří se rozhodnou pro cestu elektronického podpisu. Pokud bude o tuto službu zájem, lze předpokládat, že dojde k jejímu rozšíření a modernizaci. Může se zdát, že nabízené elektronické služby v budoucnosti povedou k omezování služeb samotných poboček veřejné správy. To ovšem bude trvat ještě mnoho let, než elektronický podpis vytlačí vlastnoruční podpis z budov institucí. Papírová komunikace bude dozajista stále využívána, jen ne v takové míře. Každý nebude mít možnost elektronicky komunikovat, proto bude vyžadovat osobní návštěvu úřadu.

3. Vymezení základních pojmů

Aby se autor mohl dále věnovat samotnému tématu práce, je nutné definovat několik důležitých termínů, které jsou v problematice „Využití elektronického podpisu pro zajištění komunikace občana s veřejnou správou“ klíčové. Jako první je vysvětlen podpis jakožto základní kámen celé komunikace. V pasáži je přiloženo schéma podpisu z pohledu využití při podepisování dokumentů. Následuje další definice toho nejdůležitějšího termínu, kterým je samotný elektronický podpis. V úvodu již byla užita základní definice, ale je nutné tento pojem dále rozšířit. Podkapitola má za úkol poskytnout několik různých definic termínu k porovnání a pomocí přiloženého schématu celý systém graficky představit. Nedílnou součástí elektronické komunikace jsou certifikáty, jakožto poskytovatelé autenticity a důkazu vlastnictví. Dále se kapitola věnuje termínům jako je elektronická podatelna, elektronická veřejná listina, elektronické časové razítko, elektronická časová značka a datová schránka. Všechny uvedené termíny jsou součástí komunikace s veřejnou správou. Na závěr je charakterizován digitální otisk, v terminologii elektronického podpisu znám jako „hash funkce“.

Podpis

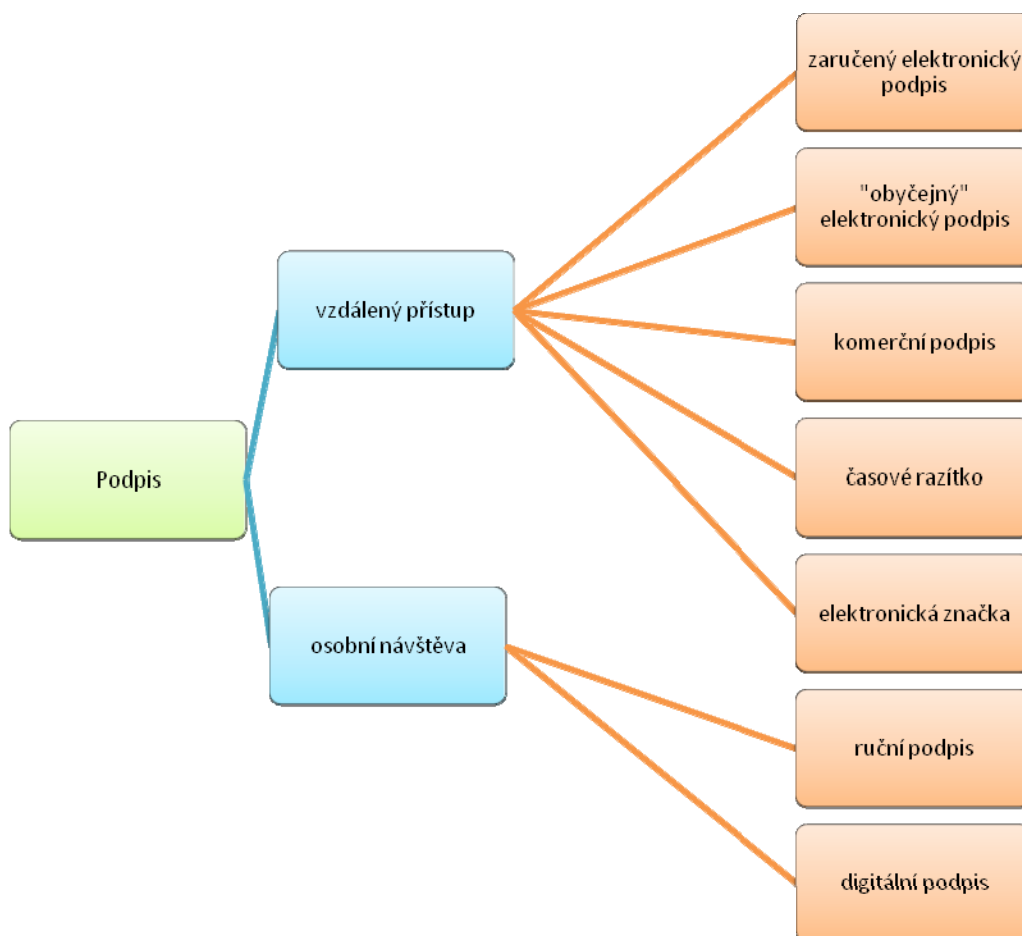
Pokud se osoba hlásí k nějakému textu, který je ve většině případů umístěn nad samotným podpisem, stvrzuje svůj souhlas nebo autorství s ním. Podpisem může být vypsání jména osoby nebo její identifikující znak.

Jeden ze způsobů, jak stvrdit svůj písemný projev (např. smlouvu), je podpis. Podpisem opatřený dokument dokládá skutečnost, že určitá osoba projevila souhlas s dokumentem, stvrdila jeho platnost, popřípadě, že se v určitou dobu nacházela na určitém místě. Občanský zákoník hovoří o podpisu jasně. Ve svém paragrafu č. 40 v odstavci 3 uvádí:

„Písemný právní úkon je platný, je-li podepsán jednající osobou; činí-li právní úkon více osob, nemusí být jejich podpisy na téže listině, ledaže právní předpis stanoví jinak. Podpis může být nahrazen mechanickými prostředky v případech, kdy je to obvyklé. Je-li právní úkon učiněn elektronickými prostředky, může být podepsán elektronicky podle zvláštních předpisů.“

Právě druhá část je pro nás důležitá. Elektronickým prostředkem je zde myšlen elektronický podpis, o kterém je celá tato práce.

Následující schéma (Obr. 3) zobrazuje užití podpisu dvěma způsoby. Kdy na jedné straně je osoba fyzicky přítomna a na straně druhé není přítomna samotnému aktu podpisu.



Obr. 3 Schéma podpisů

Elektronický podpis

Na otázku, co přesně znamená elektronický podpis, můžeme nalézt několik různých odpovědí. Existuje mnoho definic popisující tento termín z pohledu právního nebo technického. V následujících řádcích bude uvedeno několik z těchto definic, a to proto, aby byl tento termín přesně vymezen a objasněn.

V souladu se zákonem č. 227/2000 Sb., o elektronickém podpisu, se jedná o 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 (totožnosti) podepsané osoby ve vztahu k datové zprávě [Macková, 2009, s. 11].

Výše uvedená definice vychází ze Směrnice 1999/93/EC Evropského parlamentu a rady ze dne 13. prosince, o zásadách Společenství pro elektronické podpisy. V členských zemích EU je touto směrnicí řešena problematika elektronického podpisu.

Elektronický podpis je jedním z nástrojů bezpečné elektronické komunikace. Umožňuje zajistit klíčové bezpečnostní atributy spojené s důvěryhodností komunikačních systémů, tedy autentizaci komunikujících stran, průkaznost jejich kroků a integritu přenášených zpráv [Lidinský, 2008, s. 38].

Elektronický podpis je prostředek k zajištění elektronické autentizace autora (sepisovatele) a integrity podepisovaných dat. Jedná se o aplikaci schopnou s mnohem vyšší mírou důvěryhodnosti než rukou psaný podpis potvrdit nějakou skutečnost.

Elektronický podpis je též nesmírně silnou zbraní v boji proti počítačovým virům (především proti tzv. červům, které se šíří pomocí e-mailové pošty), neboť bude možné bezpečnost rozlišit, který e-mail je skutečně od odesílatele a který je podvržen k tomu, aby „vypustil“ škodlivý kód [Příbyl, 2000, s. 13-14].

Zaručený elektronický podpis

Zaručený elektronický podpis je chápán jako vyšší forma elektronického podpisu. Díky svému přesnému vymezení a vlastnostem je brán jako plnohodnotná náhrada rukou psaného podpisu. Musí ale splňovat následující požadavky:

- a) je jednoznačně spojen s podepisující osobou,
- b) umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
- c) byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
- d) je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat [Dostálek, 2006, s. 30-31].

Komerční podpis

Tento typ elektronického podpisu je vhodný pro použití v uzavřených systémech, kde je mezi účastníky bezpečné komunikace současně uzavřena smlouva, řešící mimo jiné i podmínky komunikace. V daném případě jej lze použít pro tvorbu elektronického podpisu. Je založen na komerčním certifikátu. Problematikou získání a použití zaručeného elektronického podpisu se věnují další kapitoly této práce.

Digitální podpis

Definovat tento pojem je poměrně náročné, protože panuje nesoulad mezi terminologií evropských zemí a Spojenými státy americkými. Na americkém kontinentě se pro „náš, evropský elektronický podpis vžilo označení digitální podpis. Níže uvedené definice mají za úkol přinést představu, co to je digitální podpis. Pro úplné pochopení je přiložen obrázek „evropského digitálního podpisu“, který známe například z bankovního prostředí.

Digitální podpis je podskupinou elektronického podpisu. Jedná se o bezpečnostní mechanismus, který má v zásadě sloužit jako ekvivalent „vlastnoručního“ podpisu pro užití v rámci elektronické komunikace [Macková, 2009, s. 10].

Tento podpis je vlastně číslo v desítkové či dvojkové soustavě. Od „běžných“ čísel se digitální podpis liší tím, že často bývá velké číslo (1024-2048 bitů) a že jeho výpočet nebo ověření je dosti složitý úkon, který nelze provádět ručně, ale pouze s pomocí počítače. Nemusí se ale vždy jednat o velké počítače. Ověření mohou vykonávat i miniaturní čipy, které se vejdou na čipové karty [Mates, 2006, s. 127-128].

Certifikát

Jedná se o nejdůležitější prvek stojící na samém začátku elektronického podepisování. Bez certifikátů by nebylo možné vytvořit elektronický podpis, proto je toto vysvětlení poněkud detailnějšího charakteru.

Certifikát je digitální dokument, ve kterém jsou uvedeny údaje identifikující příslušnou osobu a její veřejný ověřovací klíč [Mates, 2006, s. 135].

Certifikát je základním pilířem celého systému elektronického „podepisování“. Abychom byli schopni elektronicky „podepsat“ nějaký elektronický dokument, musíme tedy vlastnit certifikát.

K opatření vlastního certifikátu je nutné navštívit poskytovatele certifikačních služeb. V praxi najdeme pro tyto poskytovatele i jiné značení – certifikační autorita (dále jen CA). CA má v systému bezpečné elektronické komunikace pozici jakési třetí strany, která prostřednictvím vydaného certifikátu stvrdí fyzickou identitu subjektu, tedy žadatele o certifikát, s párem klíčů (elektronická identita). Jednoduše řečeno, CA vytvoří vztah páru kryptografických klíčů s jednou fyzickou osobou.

Certifikáty jsou dvojího druhu. V prvním případě je certifikát vydán nadřízenou institucí, o jejíž důvěře není pochyb. Obvykle proto, že byla zmocněna zvláštním zákonem. Za důvěryhodnost certifikátu, vydaného CA, ručí instituce, která jí certifikát vydala. Druhým, běžnějším způsobem je případ, kdy si certifikát vydá CA sama. Tyto certifikáty jsou označovány jako kořenové (někdy i jako „samopodepsané“ certifikáty). V tomto případě ale není dostatečně poskytnuta důvěryhodnost vydavatele [Budiš, 2008, s. 39-62].

Pokud se zaměříme na komunikaci s veřejnou správou, budeme vždy mluvit o kvalifikovaných certifikátech (více Kapitola 5). Jsou to tedy certifikáty prvního druhu, kdy je nadřízenou institucí zaručena důvěryhodnost a pravost.

Kvalifikovaný certifikát

Tento druh certifikátu je datová zpráva spojující data pro ověřování elektronických podpisů s podepisující, resp. označující osobou a umožňuje ověřit její identitu. Vydavatelem je kvalifikovaný poskytovatel certifikačních služeb [Macková, 2009, s. 12]. Aby mohl být kvalifikovaný certifikát užíván v oblasti veřejné správy, musí mít několik náležitostí. Tyto náležitosti jsou uvedeny v kapitole 5.

Poskytovatel certifikačních služeb

Poskytovatelem může být fyzická osoba, právnická osoba nebo organizační složka státu, která vydává certifikáty, vede jejich evidenci nebo poskytuje služby spojené s elektronickými podpisy. V případě kvalifikovaného poskytovatele certifikačních služeb, poskytovatel vydává kvalifikované certifikáty, kvalifikované systémové certifikáty, kvalifikovaná časová razítka a prostředky pro bezpečné vytváření elektronických podpisů [Macková, 2009, s. 283]. Právnímu rámci poskytovatele certifikátů se věnuje kapitola 5.

Tento poskytovatel zaručuje veřejnosti, že veřejný klíč patří opravdu tomu, kdo je označen jako vlastník. Před samotným vydáním klíče je zájemce o certifikát fyzicky identifikován.

Datová schránka

Datová schránka je elektronické úložiště, které je určeno k doručování orgány veřejné moci, k provádění úkonů vůči orgánům veřejné moci a k elektronickým úkonům mezi orgány veřejné moci navzájem [Macková, 2009, s. 10].

Tyto schránky také můžeme považovat za jakési elektronické podoby klasických poštovních schránek. Komunikace mezi subjekty je zabezpečena na základech autentizačních a autorizačních procedur. Pomocí zaručeného elektronického podpisu zde probíhá bezpečný přenos zpráv [Budiš, 2008, s. 25].

Za zřízením datových schránek byla snaha zlepšit komunikaci s veřejnou správou i uvnitř veřejné správy. Dalším přínosem by měla být úspora finančních prostředků.

Elektronická podatelna

Elektronická podatelna je pracoviště orgánu veřejné moci určené pro příjem a odesílání datových zpráv. Nejčastěji jsou podatelny využívány k poskytování informací o činnosti úřadu, jeho jednáních, rozpočtech a dalších rozhodnutích.

Elektronická značka

Elektronickou značkou se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které splňují následující požadavky:

- jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu,
- byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou,
- jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat.

Elektronické značky se budou používat tam, kde bude nezbytné důvěryhodným způsobem označovat velké objemy dat v krátkém čase. Vytváření zaručeného elektronického podpisu by pro každou zprávu bylo časově i finančně náročné. Jejich užití se počítá do agend celních řízení nebo při vydávání elektronických výpisů z úředních databází.

Elektronická veřejná listina

Písemnosti orgánů veřejné moci v elektronické podobě označené elektronickou značkou, založenou na kvalifikovaném systémovém certifikátu, vydaném akreditovaným poskytovatelem certifikačních služeb, nebo podepsané uznávaným elektronickým podpisem mají stejné právní účinky jako veřejné listiny vydané těmito orgány.

Kvalifikované časové razítko

Pomocí tohoto razítka lze důvěryhodně spojit data v elektronické podobě s časovým okamžikem a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem. Vydáním časového razítka k dokumentu je tedy zajištěno, že nemůže být později upraven a vydáván za původní. Časová razítka mají také omezenou dobu platnosti, jež je dána platností certifikátu autority časových značek.

Hash

Funkce Hash (otisk) je jednocestná funkce, která nám z libovolně dlouhého textu vytvoří krátký řetězec konstantní délky. Výsledný řetězec (otisk) by měl maximálně charakterizovat původní text. Jednocestnou funkcí se rozumí algoritmy, které nejsou výpočetně náročné. Je však výpočetně velice náročné k výsledku nalézt původní text [Dostálek, 2006, s. 21].

Díky „hash“ funkci je pak celý proces elektronického podepisování rychlejší a požadavky na bezpečnost jsou splněny.

Hash funkce by měla splňovat následující požadavky:

- odolnost vůči získání předlohy – nelze z hash hodnoty získat původní dokument,
- odolnost vůči získání jiné předlohy – nelze najít dokument, kterému by odpovídala hash hodnota jiného dokumentu,
- odolnost vůči nalezení kolize – nelze najít dva dokumenty se stejnou hash hodnotu

[Budiš, 2008, s. 34]

4. Elektronická komunikace a její bezpečnost

Tato kapitola se věnuje vysvětlením základních principů bezpečnosti elektronické komunikace. Tento typ komunikace lze chápat jako výměnu informací mezi několika subjekty prostřednictvím sdělovací techniky. Použití elektronické komunikace (např. e-mail, instant messaging) se stalo každodenní činností většiny lidí. Rozvoj v oblasti komunikačních technologií přináší velké množství způsobů, jak mohou mezi sebou komunikující strany navázat kontakt. Celý svět se stává závislým na komunikaci prostřednictvím sítí, ať jde o síť v rámci jednotlivých podniků nebo o celosvětovou síť Internet. Tyto komunikační kanály je však třeba chránit.

Žádnou komunikaci nelze provozovat bez pravidel. Ty jsou buď stanovena v závazné formě, doporučena či se alespoň jedná o obecně dodržovanou úmluvu. Pravidla komunikace se liší podle společenského prostředí, ve kterém komunikace probíhá. Odlišná pravidla platí pro společenskou, profesní či zájmovou oblast [Neugebauer, 2008].

Úkolem této části není složitý popis technologií, ale přehledné a jednoduché zpracování bezpečnostních technik při komunikaci s použitím elektronického podpisu.

4.1 Ochrana elektronické komunikace

Pokud mluvíme o elektronické komunikaci, představíme si zasílání e-mailů, chatování, používání elektronické podatelny úřadu nebo i prosté telefonování. Tyto činnosti mají své postupy a náležitosti, které komunikující strany musí plnit v rámci dosažení úrovně i zabezpečení. V době, kdy byl možný pouze písemný styk, obsah obálky nemohl být změněn, aniž by adresát změnu nezaznamenal. Princip ochrany elektronické komunikace je podobný. O obdržené zprávě musí být zřejmé, zda byla či nebyla pozměněna nepovolanou osobou.

Na otázku, proč vůbec chránit naši elektronickou komunikaci, najdeme nespočet odpovědí. Za hlavní důvod lze považovat ochranu naší osoby a našeho majetku. Není žádoucí, aby naše osobní informace byly dostupné pro veřejnost.

V souladu s mezinárodními normami lze definovat základní bezpečnostní cíle, jejichž plnění by měl důvěryhodný systém zajistit:

- **důvěrnost informací** - systém musí zabezpečit, aby přístup k důvěrným informacím měly pouze autorizované subjekty,
- **integritu** – systém musí zabezpečit informace proti modifikaci či změně přenášených dat,

- **nepopiratelnost** – systém musí mít schopnost přesvědčit třetí nezávislou stranu o přímé odpovědnosti subjektu za autorství, vlastnictví, odeslání, případně přijetí zprávy [Budiš, 2008, s. 27].

Zabezpečení musí řešeno u odesílatele a adresáta, nebo někde na cestě mezi nimi. Tyto komunikační cesty jsou vlastně kanály elektronické komunikace. Ochránit tyto kanály je však velký problém. Při elektronické výměně informací jsou využívány kabelové linky nebo bezdrátové technologie.

Ochrany komunikace jsou realizovány:

- ochranou přenosové sítě
- ochranou u odesílatele a adresáta šifrování

Ochrana přenosové sítě

Přenosovou síť lze chránit fyzickou přítomností lidí. To je ovšem značně nereálné řešení. Dalším způsobem fyzického zabezpečení by byla situace, kdy by náš počítač nebyl vůbec připojen do komunikační sítě. Absence připojení však znemožní samotnou elektronickou komunikaci.

Ochrana u odesílatele a adresáta

Druhý způsob ochrany působí samozřejmě reálněji než předchozí metoda. Jednoduchá ochrana u komunikujících subjektů je docílena omezením přístupů k danému počítači či kanceláře. V současnosti se však nabízí moderní ochrana dat pomocí jejich zašifrování. Zvolenou metodou lze zasláná data ochránit v takové míře, že se elektronická komunikace mezi subjekty bude rovnat komunikaci osobního styku. Z tohoto důvodu se dnes se šifrováním setkáváme doslova na každém kroku. Otázka šifrování je vysvětlena níže.

4.2 Šifrování

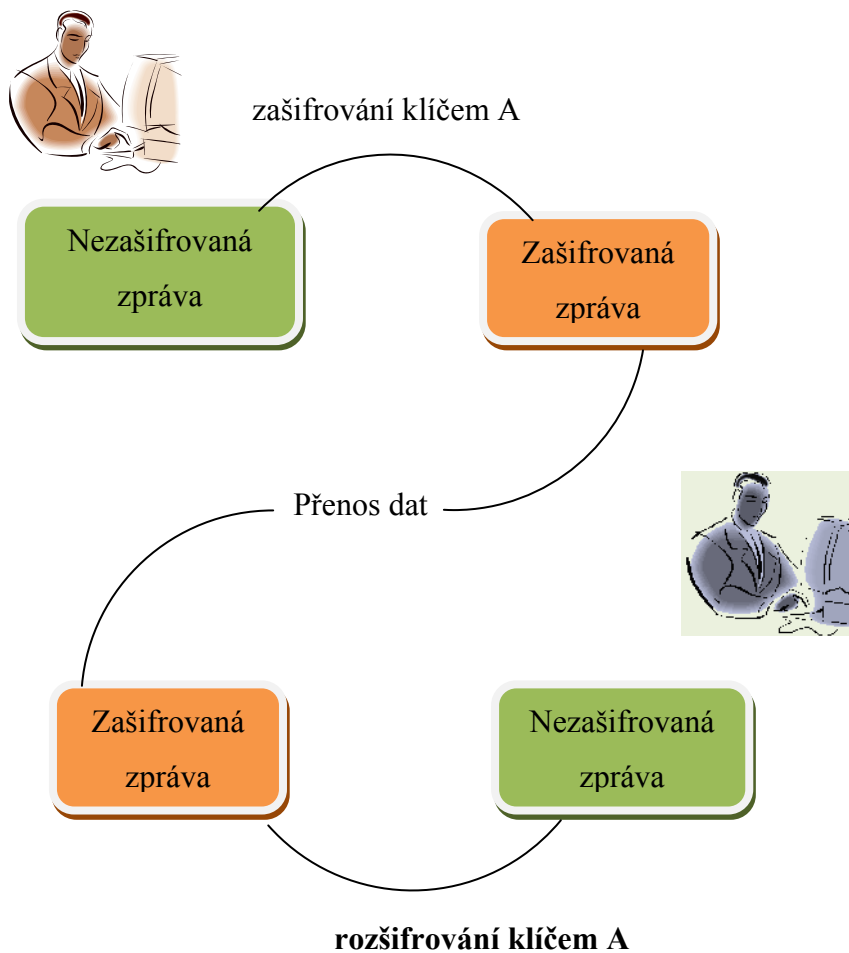
Šifrování neboli kryptografie je nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí tzv. klíče. Metoda šifrování je základním prvkem technické stránky elektronického popisu.

Rozlišují se dva základní druhy kryptografie:

- **symetrická**
- **asymetrická**

Symetrická kryptografie

Metoda symetrické kryptografie (Obr. 4) využívá k zašifrování zprávy jeden šifrovací klíč. Tento klíč používá jak odesílatel zprávy, tak i adresát. V tomto případě je tedy nutné, aby si strany bezpečným způsobem vyměnily šifrovací klíč.



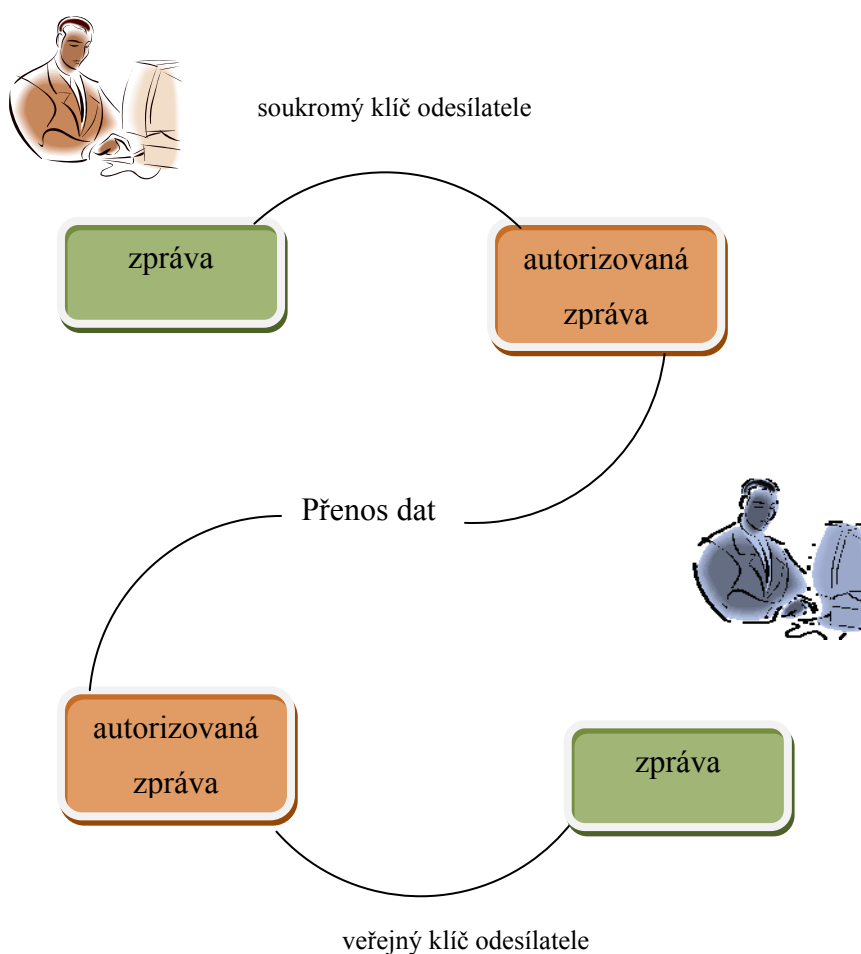
Obr. 4 Šifrování symetrickou šifrou

Asymetrické kryptografie

Asymetrická kryptografie (Obr. 5) se vyznačuje užitím dvojice klíčů. V odborné literatuře se také setkáváme s termínem „párová data“. Dvojici klíčů si uživatel vygeneruje sám pomocí běžně dostupného softwaru. Je tedy jejich jediným vlastníkem. První klíč je označován jako podepisující, soukromý nebo tajný. Slouží k zašifrování zprávy. Druhý z páru

klíčů se nazývá veřejný a slouží k rozšifrování. Veřejný klíč lze zveřejnit, protože z něj nejde v reálném čase odvodit podepisující klíč. Tento způsob se označuje jako kryptografie s veřejným klíčem.

Princip spočívá v tom, že data šifrovaná jedním z klíčů lze v rozumném čase dešifrovat pouze se znalostí druhého klíče a naopak. Zpráva je zašifrována privátním klíčem. Protože je veřejný klíč obecně znám všem, není problém pro adresáta zprávu dešifrovat a získat tak identitu odesílatele. Tato zpráva však není považována za důvěrnou, ale pouze za autorizovanou (nepopíratelnou). To je vlastní princip elektronického podpisu [Budiš, 2008, s. 30].



Obr. 5 Asymetrické šifrování

4.3 Typy úrovně ochrany zpráv pomocí šifrování

Při použití elektronického podpisu nemusí docházet k zašifrování zprávy. V této části jsou uvedeny tři stupně ochrany, které se používají v praxi. Jejich výběr záleží na požadavcích uživatele a na rychlosti komunikace.

Tři stupně ochrany:

- neadresovaná, nezašifrovaná, ale autorizovaná zpráva
- adresovaná, zašifrovaná, ale neautorizovaná zpráva
- adresovaná, zašifrovaná a autorizovaná zpráva

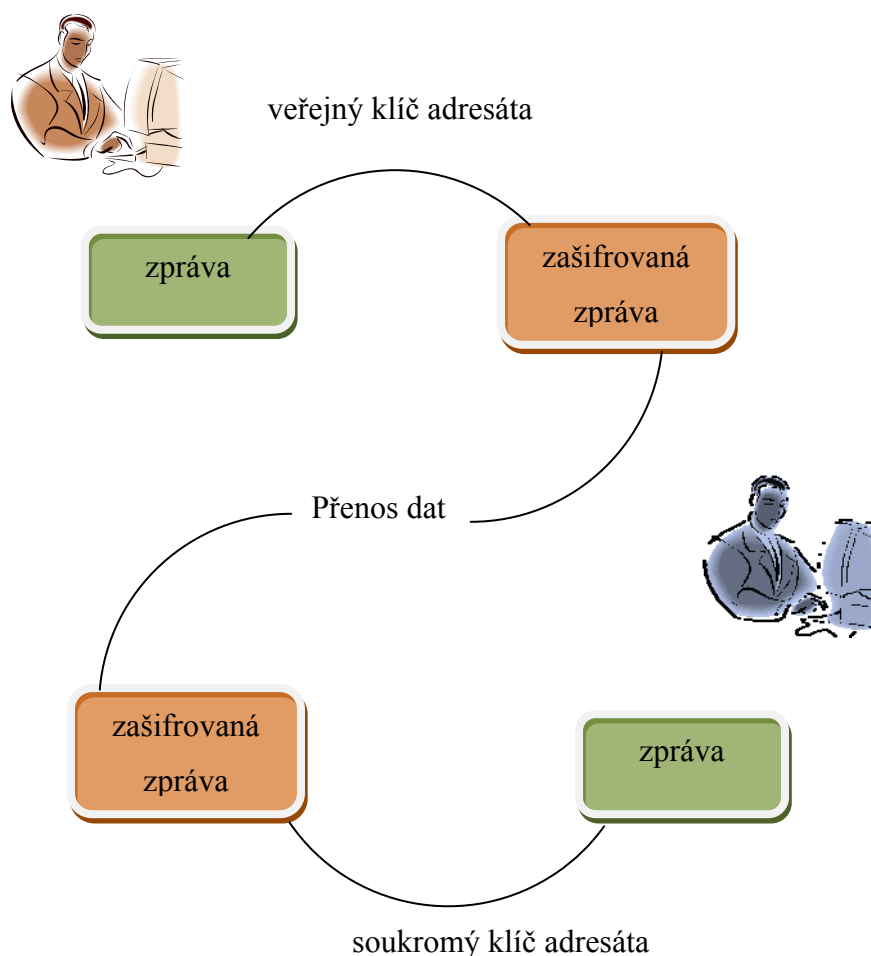
I. Neadresovaná, nezašifrovaná, ale autorizovaná zpráva

Zpráva je šifrována soukromým klíčem a příjemce zprávy má k dispozici odpovídající veřejný klíč, kterým lze zprávu dešifrovat, tedy určit odesílatele. Protože je veřejný klíč znám všem, nelze soukromým klíčem šifrovanou zprávu považovat za zašifrovanou v plném slova smyslu, ale pouze za nepopíratelnou. To je princip celého elektronického podpisu. Celý proces je opět graficky znázorněn na obr. 5.

Tento způsob však nesplňuje bezpečnostní podmínku důvěrnosti zprávy, protože zpráva sama o sobě neobsahuje ochranu proti přečtení třetím neautorizovaným subjektem. Zprávu si může přečíst kdokoli, kdo zprávu získá. Zpráva obsahuje jen důvěryhodný podpis odesílatele zprávy.

II. Adresovaná, zašifrovaná, ale neautorizovaná zpráva

K zajištění důvěrnosti odeslané zprávy se používá šifrování zpráv pomocí veřejného klíče adresáta. Tento postup (Obr. 6) se také označuje jako „vkládání do elektronické obálky“. V tomto případě má odesílatel jistotu, že zprávu si přečte jen adresát zprávy, protože vlastní soukromý klíč (druhý z páru), který „otevře“ elektronickou obálku.



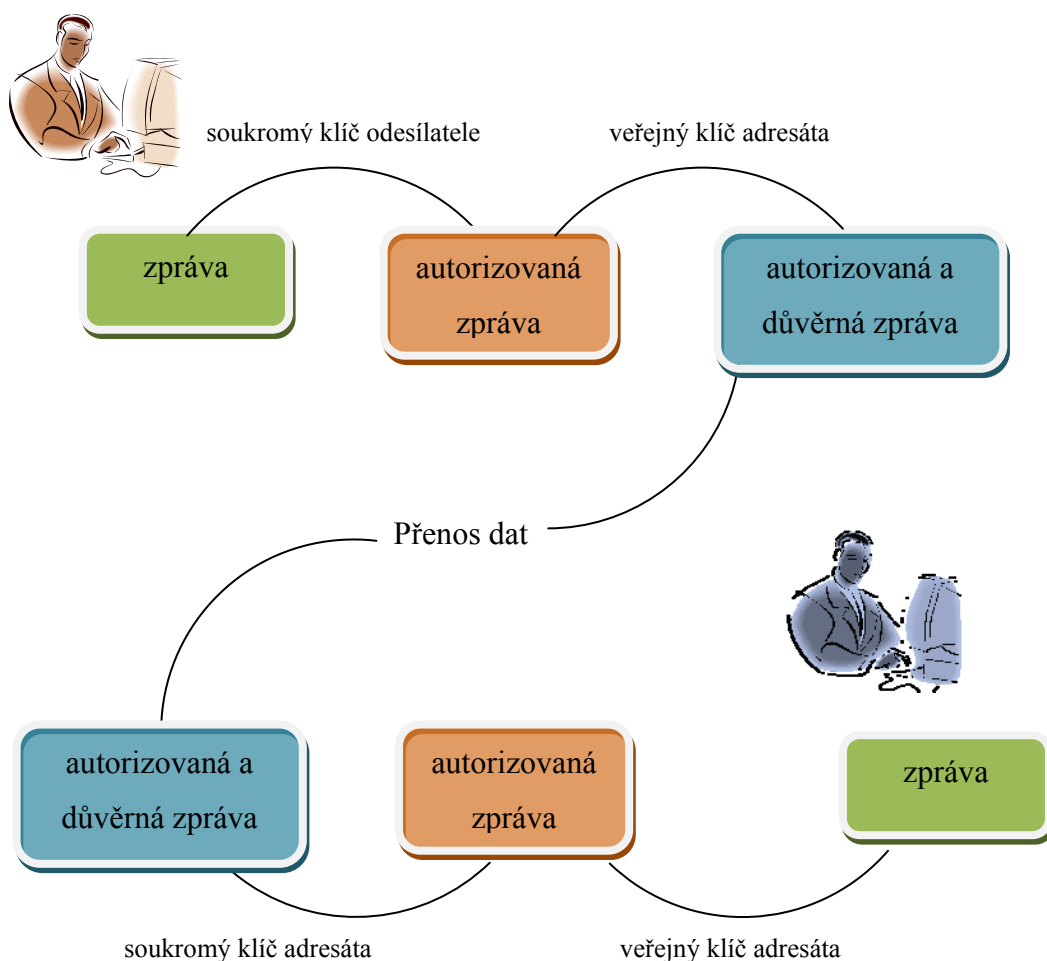
Obr. 6 Adresovaná, zašifrovaná, ale neautorizovaná zpráva

V tomto případě však není splněna podmínka nepopíratelnosti zprávy, protože zpráva není opatřena identifikujícím podpisem odesílatele.

III. Adresovaná, zašifrovaná a autorizovaná zpráva

Tento způsob (Obr. 7) popisuje zašifrování i podepsání zprávy, tedy nejbezpečnější způsob, jakým lze zaslat zprávu.

Zpráva je na začátku podepsána soukromým klíčem odesílatele. Podepsaná zpráva je poté zašifrována veřejným klíčem adresáta. Tím je plně zajištěna integrita, nepopíratelnost a důvěrnost zprávy. První krok příjemce je dešifrování zprávy svým soukromým klíčem. Následuje rozšifrování pomocí veřejného klíče odesílatele, čímž se dosáhne ověření jeho identifikace a současně je získán čitelný text zprávy [Budiš, 2008, s. 32-33].



Obr. 7 Adresovaná, zašifrovaná a autorizovaná zpráva

4.4 Právní ochrana

V širším pohledu na zabezpečení elektronického podepisování, je dobré zohlednit, že ochranou musíme chápat i právní zabezpečení veřejné správy. Hlavním zákonem v této oblasti je zákon č. 227/2000 Sb., o elektronickém podpisu (vice Kapitola 5). V následující pasáži je charakterizován zákon vymezující systém eGovernmentu, který se významně podílí na službách elektronické veřejné správy.

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy

Zákon o informačních systémech veřejné správy stanoví práva a povinnosti správců informačních systémů veřejné správy (dále jen ISVS) a dalších subjektů, jež souvisejí s vytvářením, užíváním, provozem a rozvojem informačních systémů veřejné správy. V návaznosti na to upravuje působnost Ministerstva informatiky jako ústředního správního

úřadu pro tvorbu a rozvoj informačních systémů veřejné správy. Zákon vytváří podmínky, aby kvalitní informační systémy byly dobrým nástrojem pro výkon veřejné správy.

Zákon dále mj. upravuje atestace ISVS a postavení atestačních středisek, doručování zpráv orgánům veřejné moci prostřednictvím portálu veřejné správy a poskytování ověřených výstupů z ISVS.⁷

Novela tohoto zákona proběhla zákonem č. 81/2006 Sb., který reagoval na rozvoj informačních a komunikačních technologií a poskytovala základ pro další postupné zavádění služeb eGovernmentu.

Zákon nově upravoval služby a úkoly portálu veřejné správy. Novela umožňuje, aby datová zpráva podepsaná zaručeným elektronickým podpisem a odeslaná prostřednictvím portálu veřejné správy, mohla být považována za doručenou úřadu, kterému byla adresována. Tato změna pomohla k dalšímu rozvoji rychlé a méně nákladné komunikace se státem.

Další důležitou částí novely byla povinnost přizpůsobit webové stránky institucí veřejné správy a samosprávy tak, aby byly přístupné i pro osoby zdravotně postižené. Tato povinnost byla zavedena od 1. ledna 2008 [Česko, ©2010e].

4.5 Užití v praxi

V praxi se zpravidla při tvorbě elektronického podpisu nešifruje soukromým klíčem odesílatele celá zpráva, ale použije se tzv. **hash funkce** (více Kapitola 2). Použitím této funkce vznikne hodnota o pevné délce (tzv. hash hodnota), jenž je výsledkem zhuštění samotné zprávy.

Tato hodnota je pak zašifrovaná asymetrickou metodou s použitím soukromého klíče. Tím vzniknou data pro vytvoření elektronického podpisu. Výsledek je pak odeslán společně se zprávou jako příloha nebo je umístěn do samostatného bloku.

Kontrola podpisu pak probíhá tak, že adresát pomocí stejného algoritmu vypočte novou hash hodnotu zprávy a tu pak porovná s již dešifrovanou hodnotou přiloženou ke zprávě jako příloha [Budiš, 2008, s. 30]. Obě hodnoty se musí rovnat, aby nastala shoda, což potvrzuje platnost a důvěryhodnost elektronického podpisu.

⁷ Zákonem č. 365/2000 Sb. byla definice informačního systému mírně pozměněna na toto znění: *Informačním systémem se rozumí funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost. Každý informační systém zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, a dále nástroje umožňující výkon informačních činností.*

Další možností, která se pro svou rychlost využívá více, je postup, kdy dochází i k symetrickému šifrování. Užití tohoto postupu se používá například v elektronické poště (e-mail).

Odesílatel zprávy nejprve vypočte hash hodnotu a tu zašifruje svým soukromým klíčem. Tím vznikne elektronický podpis zprávy. Potom zprávu zašifruje veřejným klíčem adresáta, čímž bude zpráva nečitelná neautorizovanými subjekty.

Adresát přijatou zprávu nejprve dešifruje za pomoci svého soukromého klíče. Podpis ověří výpočtem hash hodnoty zprávy a jejím srovnáním s dešifrovanou hash hodnotou z elektronického podpisu. Pokud dojde ke shodě, je zpráva považována za bezpečnou.

Protože využití asymetrického algoritmu požadavku na důvěryhodnost je časově náročné, častěji se používá model, kdy je asymetrická metoda využita pouze k tvorbě elektronického podpisu a bezpečné výměně klíčů pro symetrickou kryptografii, která je užitá k zašifrování přenášených dat zprávy. Pro každou zprávu pak lze vygenerovat nový symetrický klíč, který bude určen k zajištění důvěrnosti zprávy. Samotný klíč je poté šifrován veřejným klíčem adresáta, čímž je zaručeno, že se k tomuto klíči dostane jen adresát, který ho užije k dešifrování zprávy [Budiš, 2008, s. 35-37].

4.6 Problémy bezpečnosti elektronické komunikace

Za největší problém v procesu šifrování elektronické komunikace je považována správa kryptografických klíčů. Pokud by si jednotlivé subjekty nehlídaly své klíče, mohlo by dojít k prolomení ochrany a poškození dat. Jestliže jsou všechna bezpečnostní pravidla pro ochranu klíčů dodržována, je šifrování jeden z neúčinnějších způsobů, jak chránit svá data.

Pokud se zaměříme na další slabé články bezpečnosti, je nutné zmínit ochranu prohlížečů internetových stránek. Pro docílení co možná největší bezpečnosti je nutné instalovat bezpečnostní záplaty, které zpravidla vydává tvůrce prohlížeče. Pravidelnou aktualizací prohlížečů se zvyšuje úroveň zabezpečení. Na adrese www.datoveschranky.info (Příloha č. 1) jsou publikována varování ohledně možných rizik spojených používáním datových schránek. V sekci „Bezpečnost“ lze najít bezpečnostní desatero uživatele [Smolík, 2010, s. 33].

Bezpečnost komunikace však záleží vždy na člověku. V případě bankovní komunikace je za méně bezpečnou část řetězce považován uživatel. Bankovní instituce má zabezpečení svého systému na vysoké úrovni. Uživatel, který však nedisponuje takovými ochrannými prostředky, se snadno stane terčem útoku. Ke zvýšení bezpečnosti komunikace tak znatelně

přispívá více-faktorová autorizace, při níž je například využito autorizačních bankovních SMS zpráv. Uživateli je po zadání jména a hesla odeslána SMS zpráva s jedinečným kódem pro přístup ke svému účtu [Rašek, 2006]

V odborné společnosti najdeme také názory, že použití elektronického podpisu u úředního dokumentu je „průšvih“. I když elektronický podpis u nás funguje od roku 2000, najde se stále dost lidí i úředníků, kteří jej neumí správně a bezpečně používat. Pak se nelze divit tomu, že si tito lidé neuvědomují bezpečnostní rizika. S příchodem datových schránek rapidně poroste počet lidí (úředníci i občané), co se s elektronickým podpisem bude velmi často setkávat. Každý úředník i pracovník, který někdy bude muset přijímat dokumenty opatřené elektronickým podpisem, by měl být dostatečně proškolen, aby rozpoznal platnost podpisu dokumentu [Vystavělová, 2009, s. 40-41].

Velké nebezpečí spojené s elektronickou komunikací je tzv. **phishing**. Jedná se o způsob získávání osobních údajů, většinou v oblasti elektronického bankovníctví. Jeho podstatou je nejprve získání informací o způsobech komunikace banky s klientem. Následuje podvržený e-mail od narušitele, jnež jménem dané banky informuje zákazníka o změně systému zabezpečení komunikace a požaduje od klienta zaslání přístupového jména, hesla a čísla účtu. Pak dojde k vyčerpání bankovního konta.

Závěrem lze říci, že trendem moderní doby bude elektronická komunikace, její podepisování a šifrování. Čím dál více institucí bude nabízet své služby přes internetovou síť, proto i úroveň bezpečnosti bude stoupat. Vývoj technologií do jisté míry určuje způsoby komunikace, základu společnosti. Pokud nebudou hlídána naše data, může nastat zmatek, kterého se západní země natolik bojí, že věnují nemalé částky na zabezpečení elektronické komunikace. Informace se stávají velmi cennou obchodní komoditou, stejně jako např. zlato.

5. Právní rámec pro využití elektronického podpisu v elektronických dokumentech

Níže je charakterizován zákon o elektronickém podpisu a jeho okolnosti. Jako první jsou uvedeny vzorové legislativní dokumenty Komise UNCITRAL pokládající základní kámen všech následujících zákonů. Následuje důležitá směrnice Evropského parlamentu a Rady, která znatelně ovlivnila český zákon o elektronickém podpisu. Pokračuje hlavní část charakterizující klíčový zákon č. 227/2000 Sb. Další podkapitola obsahuje shrnutí dvou dalších dokumentů znatelně ovlivňujících právní rámec elektronického podpisu v České republice. Jedná se o vyhlášku č. 378/2006 Sb. a o nařízení vlády č. 495/2004 Sb. V závěru kapitoly jsou uvedeny názory odborné veřejnosti hodnotící českou legislativu. V příloze č. 2 je uveden seznam veškerých zákonů, které se zabývají touto problematikou.

5.1 Komise UNCITRAL

Abychom našli prvopočátky legislativy elektronického podpisu, je na místě se zmínit o Komisi UNCITRAL⁸. Komise vydala několik dokumentů týkajících se mezinárodního obchodu, ale zabývala se i otázkou bezpečné elektronické komunikace a výsledkem byly tyto dokumenty:

- a) Doporučení UNCITRAL, týkající se právní závaznosti elektronických údajů (1985),
- b) Vzorový zákon UNCITRAL o elektronickém obchodu (1996),
- c) Vzorový zákon o elektronickém podpisu (2001).

Z pohledu vývoje legislativního rámce elektronického podpisu bylo předloženo vzorového zákona o elektronickém obchodu a následné schválení Valným shromážděním OSN v roce 1996. Zákon obsahuje pasáž řešící užití elektronického podpisu.

První část zákona je zaměřena na terminologický základ, hlavní pojmy a definice. Druhá část je vedena jako průvodce k ustanovení zákona o elektronickém podpisu. Jsou zde například popsány přístupy ohledně účelu zákona či harmonizaci práva [Budiš, 2008, s. 99-102].

⁸ UNCITRAL se zaměřuje na sjednávání vzorových předpisů, mnohostranných mezinárodních úmluv, legislativních doporučení apod. s cílem napomoci odstranění právních překážek mezinárodního obchodu [Česko, ©2010c].

5.2 Směrnice 1999/93/ES

V evropském měřítku vznikla směrnice EU, jejímž cílem bylo standardizovat prostředí bezpečné elektronické komunikace v rámci zemí Evropské unie. Směrnice 1999/93/ES Evropského parlamentu a rady o zásadách Společenství pro elektronické podpisy byla přijata 13. prosince 1999. Směrnice se zabývá použitím elektronického podpisu pro určení identifikace nebo obchodování. Dále pak doporučuje, jak a čím by se měly členské země řídit. Popisuje procesy vydávání certifikátů a služby poskytovatelů.

5.3 Zákon 227/2000 Sb., o elektronickém podpisu

Tato pasáž se bude věnovat nejdůležitějšímu legislativnímu dokumentu. Vymezuje problematiku elektronického podpisu, tedy zákonu 227/2000 Sb., o elektronickém podpisu. Nejprve je uveden přehled novel tohoto zákona (Obr. 8), protože během působení zákona došlo k mnoha jeho změnám. Následuje úvod k samotnému zákonu. V další části jsou detailně charakterizovány jednotlivé problematiky, kterými se tento zákon věnuje. Tyto pojmy byly již definovány v kapitole 2. Tato kapitola se však na ně zaměřuje z pohledu práva.

Tabulka č. 1 Novelý zákona č. 227/2000 Sb.

Přehled novel zákona č. 227/2000 Sb., o elektronickém podpisu.		
	zákon č. 226/2002 Sb.	
	zákon č. 517/2002 Sb.	
	zákon č. 440/2004 Sb.	
	zákon č. 635/2004 Sb.	
	zákon č. 501/2004 Sb.	
	zákon č. 444/2005 Sb.	
	zákon č. 110/2007 Sb.	
	zákon č. 124/2008 Sb.	
	zákon č. 190/2009 Sb.	
	zákon č. 223/2009 Sb.	
	zákon č. 227/2009 Sb.	
	zákon č. 281/2009 Sb.	
	zákon č. 101/2010 Sb.	

Zákon o elektronickém podpisu musel vzniknout z několika důvodů. Orgány státní správy, které dnes využívají tuto technologii, mohou dle zákonů dělat pouze to, co jim platné

zákony umožňují. Jako další důvod můžeme uvést podmínku pro vstup České republiky do Evropské unie.

Česká republika byla jedna z nejrychlejších zemí Evropy, které zareagovaly na vydání evropské směrnice EU č. 1999/93/EC z roku 1999 o zásadách Společenství pro elektronické podpisy. Výsledkem této reakce byl právě tento zákon o elektronickém podpisu. Jeho přínos není jen v technické rovině, ale ve skutečném revolučním proniknutí elektroniky do hájemství tradičního papírového dokumentu. Zákon totiž zrovnoprávňuje papírové a elektronické dokumenty a podání učiněná nejružnějšími orgánům. Přijetí zákona také doplnilo občanský zákoník v ustanoveních § 40, týkajících se písemných právních úkonů a podepisování o tuto větu:

„Právní úkon, učiněný elektronickými prostředky, může být podepsán elektronicky podle zvláštních předpisů.“

Zákon č. 227/2000 Sb. definuje klíčové pojmy, postupy a subjekty práva účastníci se na vytváření, používání a ověřování elektronických podpisů a zaručených elektronických podpisů jako prostředků umožňujících používání elektronických dokumentů způsobem v souladu s obecně závaznými právními normami. Snahou předkladatelů bylo, aby zákon byl co nejobecnější a co nejméně závislý na použitých technologiích, protože nebude při každé změně technologie potřeba měnit text zákona [Mates, 2006 s. 144-146].

Technologie se v dnešní době mění v řádech měsíců či roků. S legislativními dokumenty to, bohužel, není stejné.

5.3.1 Jednotlivá témata zákona č. 227/2000 Sb.

Povinnosti podepisující osoby

Osoba opatřující dokument elektronickým podpisem musí zabránit neoprávněné osobě v použití svého podpisu. Pokud se vyskytne nebezpečí, že by daný certifikát mohl být zneužit, podepisující osoba je povinna kontaktovat svého poskytovatele certifikačních služeb, a ten daný certifikát zneplatní. V případě, že nepovolaná osoba použije cizí elektronický podpis a tím vzniknou škody, je odpovědná osoba vlastníci daný certifikát.

Další povinností této osoby je uvádět vždy pravdivé údaje poskytovateli svých certifikačních služeb. Pokud se údaje změni, musí držitel neprodleně informovat svého poskytovatele. Všechny tyto zásady platí také pro subjekt, který opatřuje dokument elektronickou značkou (více Kapitola 3).

Kvalifikovaný poskytovatel certifikačních služeb

Tento pojem byl již uveden v kapitole 3. Následující pasáž danou problematiku rozšiřuje.

Mezi povinnosti kvalifikovaného poskytovatele patří povinnost zajistit jednoznačnou identifikaci majitele kvalifikovaného certifikátu nebo razítka. §6 zákona 227/2000 Sb. také ukládá povinnost zajistit odborné pracovníky pracující s kvalifikovanými certifikáty. Pracoviště poskytovatele musí být vybaveno náležitými bezpečnostními systémy, jako jsou např. kryptografické nástroje, nebo bezpečná úložiště kvalifikovaných certifikátů.

Smlouvu o certifikačních službách musí kvalifikovaný poskytovatel se zájemcem podepsat v písemné formě. Následně pak uchovává smlouvu, žádost o poskytování služeb, certifikát, kopie předložených osobních dokladů podepisující osoby nebo dokumenty související s životním cyklem certifikátu.

Poskytovatel je odpovědný za správnost všech údajů uvedených v certifikátu. Pokud by došlo k narušení bezpečnosti certifikátů, musí je poskytovatel neprodleně zrušit, aby se zabránilo zneužití.

V následujících případech musí poskytovatel zneplatnit kvalifikovaný certifikát:

- úmrtí držitele certifikátu,
- zániknutí držitele v případě právnické osoby,
- soud zbaví či omezí držiteli způsobilost k právním úkonům,
- změna údajů, na jejichž základě byl certifikát vydán.

Akreditace a dozor nad certifikačními službami

Akreditaci kvalifikovaného poskytovatele zajišťuje Ministerstvo vnitra České republiky. To také zveřejňuje akreditované poskytovatele. V současnosti mají danou akreditaci tři následující subjekty:

- **První certifikační autorita, a.s.,**
- **Česká pošta, s.p.,**
- **eIdentity, a.s.**

Službami těchto poskytovatelů se věnuje kapitola 6.

Ministerstvo také vede evidenci vydaných certifikátů a také je zveřejňuje (více Kapitola 4). Také může udělit při nedodržení povinností kvalifikovanému poskytovateli certifikačních služeb pokut do výše 10 000 000 Kč. Ministerstvo též může poskytovateli nařídit, aby ve stanovené lhůtě odstranil své nedostatky. Pokud tak neučiní, dojde k odebrání akreditace. Tím by došlo i k zneplatnění certifikátů vydaných v době působnosti poskytovatele.

Certifikáty

Jedinými certifikáty, které lze užít při komunikaci s úřady, jsou kvalifikované certifikáty vydané kvalifikovaným poskytovatelem. Novelizací zákona č. 227/2000 Sb. byl zákon č. 227/2009 Sb., který nabýval účinností k 1. červenci 2010. Zákon přinesl dodatek, kdy lze akceptovat zaručené elektronické podpisy založené na kvalifikovaných certifikátech vydaných kvalifikovaným poskytovatelem, který pochází z některých zemí EU.

Mezi hlavní náležitosti kvalifikovaného certifikátu patří:

- označení, dle kterého je vydán (resp. dle zákona č. 227/2000 Sb.),
- jméno, popřípadě jména a příjmení podepisující osoby nebo její pseudonym s příslušným označením, že se jedná o pseudonym, data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby,
- elektronickou značku poskytovatele certifikačních služeb,
- číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb,
- počátek a konec platnosti certifikátu,
- omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít.

Prostředky pro vytváření a ověřování elektronických podpisů

Tyto prostředky musí za pomoci technických a programových nástrojů zajistit tyto hlavní body:

- data pro vytváření podpisu se mohou vyskytnout jen jednou a jejich utajení je zajištěno,
- chránit podpis proti padělání,
- nesmí měnit data, která se podepisují,
- musí zabezpečit spolehlivé ověření podpisu,

- výsledek ověření a totožnost podepisující osoby byly řádně zobrazeny.

Elektronická značka a elektronická veřejná listina

V roce 2004 došlo k novelizaci zákona č. 227/2000 Sb. zákonem č. 440/2004 Sb., který zavedl další dvě novinky – elektronická značka a elektronická veřejná listina (více Kapitola 3).

Elektronickou značkou nelze právně chápat jako elektronický podpis, protože označující osoba označila datovou zprávu bez předchozí kontroly vlastního obsahu datové zprávy. U elektronického podpisu to je naopak. Elektronickou značku může mít k označení dat i právnická osoba nebo organizační složka státu, a to automatizovaně.

Elektronické veřejné listiny, založené na kvalifikovaném systémovém certifikátu, jsou způsobilé zajistit nepopiratelnost a originalitu dokumentu. Tyto listiny mají tedy stejnou váhu jako „klasické“ listiny označené úředním razítkem a podpisem úřední osoby.

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

Vyhláška se vztahuje na poskytovatele certifikačních služeb. Formuluje povinnosti kvalifikovaných poskytovatelů při vydávání kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek. Poskytovatel musí zajistit, aby prostředky pro bezpečné vytváření elektronických podpisů byly připraveny a předány uživateli v souladu s bezpečnostními a funkčními požadavky standardu pro důvěryhodné systémy. Poskytovatel se také může řídit technickou a uživatelskou dokumentací výrobce nebo dodavatele.

Hlava druhá je věnována požadavkům na ochranu soukromých klíčů. Ty se používají při vytváření elektronických značek a vztahují se na označující osoby, zejména pro orgány veřejné moci.

Vyhláška obsahuje 2 přílohy. Příloha č. 1 této vyhlášky obsahuje standardy a normy zaměřené na technologii certifikátů, elektronických podpisů, časových razítek nebo na kryptografické postupy. Přílohou č. 2 vyhlášky je struktura certifikační politiky a certifikační prováděcí směrnice.

Cílem této vyhlášky je technická standardizace, vymezení požadavků na bezpečnost systémů a na zpracování bezpečnostní dokumentace při poskytování certifikačních služeb.

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

Vydání nařízení lze považovat za přelomové v celém systému elektronické veřejné správy. Odstartovalo moderní trend komunikace, který je v ostatních zemích EU velmi rozšířen. Jako přínos lze označit fakt, že držitel zaručeného elektronického podpisu může komunikovat s úřady veřejné správy z domova, a to podstatně rychleji⁹.

Zřízení elektronických podatelny je povinnost orgánů veřejné moci vyplývající ze zákona č. 227/2000 Sb., §11 odst. 3, které také vymezuje zřízení podatelny. Toto nařízení je určeno pro orgány veřejné moci, které mají povinnost přijímat a odesílat datové zprávy se zaručenými elektronickými podpisy založenými na kvalifikovaných certifikátech prostřednictvím elektronické podatelny. Nařízení obsahuje zásady, kterými by se měly orgány veřejné moci řídit.

V §1 se také nařizuje, aby orgán veřejné moci vybavil elektronikou podatelnu technickým a softwarovým vybavením potřebným k chodu podatelny. Dále musí být zaměstnanci vybaveni kvalifikovanými certifikáty od akreditovaných poskytovatelů certifikačních služeb. Toto se vztahuje na zaměstnance, kteří jsou oprávněni vykonávat právní úkony. Pokud je objem došlých datových zpráv malý, je dovoleno, aby se tento orgán dohodl s jiným orgánem veřejné správy na převzetí provozu podatelny.

§3 nařízení dále upravuje činnost orgánů v oblasti zveřejňování informací ohledně přístupu a chodu elektronické podatelny. Například musí být zveřejněna elektronická adresa elektronické podatelny, nebo způsob vyřizování dotazů týkajících se provozu elektronické podatelny.

5.6 Shrnutí

V následujících řádcích práce využívá názory odborníků, kteří se svými příspěvky v internetových fórech nebo články vyjádřili k této problematice.

⁹ Na toto nařízení vlády navazuje vyhláška č. 496/2004 Sb., k elektronickým podatelnam. Upravuje postup, jak by měly orgány přijímat a odesílat datové zprávy pomocí elektronické podatelny. Příloha vyhlášky obsahuje postup nutný k ověření platnosti zaručeného elektronického podpisu, elektronického razítka, elektronické značky, kvalifikovaného certifikátu a kvalifikovaného systémového certifikátu. Tato vyhláška je také označována jako návod pro úřady veřejné správy.

Jako závažný problém, který omezuje širší uplatnění této technologie, je označováno mezinárodní uznávání elektronického podpisu. Členské země totiž mohou na základě Směrnice Evropského parlamentu a Rady 1999/93/ES používání elektronického podpisu ve veřejné správě podmínit případnými doplňujícími požadavky. Proto může nastat problém, když občan země EU použije svůj zaručený elektronický podpis v jiné členské zemi [Budiš, 2008, s. 144-147].

Zaručený elektronický podpis může přinést nové postupy a možnosti při komunikaci s veřejnou správou. Dnes totiž vzniká eventualita styku s veřejnou správou, kdy místo návštěvy úřadů lze vše vyřídit pomocí elektronického podpisu. Jako další kladný přínos zákona 227/2000 Sb. označují odborníci „skrytou“ novelizaci všech hlavních procesních právních norem (občanského soudního řádu, správního řádu, trestního řádu, a zákona o správě daní a poplatků), ve kterých byla vymezena možnost elektronického podání.

Elektronický podpis může také přinést větší průkaznost finančních transakcí, kdy by mohla vzrůst důvěryhodnost všech operací. To si lze představit i internetovém obchodování, kdy by provozovatel obchodu mohl přijímat objednávky opatřené elektronickým podpisem. Měl by tak jistotu, že uvedené údaje jsou pravdivé. V případě porušení smluvních podmínek by bylo také možné snáze identifikovat kupujícího.

Zajímavé názory přinesl článek Jiřího Peterky. Autor se věnuje problému definování digitálního a elektronického podpisu. Chybou evropských zákonodárců, kteří tvořili směrnici EU o elektronickém podpisu, bylo prosazení změny z původního termínu digitální podpis na elektronický podpis [Peterka, 2000].

Experti hodnotící elektronické podepisování se shodují v jedné věci. Internet je rozšířen v celém světě. Má svoje klady a zápory. Největším záporem internetové komunikace je anonymita zúčastněných stran. Díky elektronickému podpisu by pak byla možná komunikace (např. chatování, obchodování) mezi subjekty, které by si byly naprosto jisty identitou druhé strany.

Odborná veřejnost se zatím neshodla na otázce, zda v zákoně definovat technické normy, dle kterých by se mělo postupovat při elektronické komunikaci. V současnosti se v zákonech neuvádějí technické normy, protože vývoj technologií je velmi rychlý. Změna technologií by pak vyžadovala změnu v legislativě. Ovšem náležitosti legislativních procesů neumožňují pohotovou reakci. Přítomnost technických směrnic by však vedla ke standardizaci celého procesu a ke zvýšení bezpečnosti. V této chvíli však vítězí obecnější znění zákonů.

Přínosem legislativy je jistě prolomení bariéry jedinečnosti klasického vlastnoručního podpisu dokumentu v papírové formě. Stovky let fungoval podpis jako záruka všech smluv, zákonů či jako identifikace autorství. Pokrok doby přinesl možnost elektronického podepisování dokumentů v elektronické podobě. Dle §40 Občanského zákoníku, si jsou papírové i elektronické podpisy právních úkonů rovné. Když tuto možnost máme, musíme ji využít v co nejširším rozsahu. Můžeme tak ušetřit svůj čas i finanční prostředky.

Na závěr je nutno dodat, že systém elektronické komunikace s veřejnou správou je stále systémem novým. Nejde o procesy a postupy, které fungují desítky let. To samozřejmě přináší stále nové poznatky a zkušenosti, proto jsou změny v legislativě na místě. Pokud by se legislativa nepřizpůsobovala rozvoji technologie elektronické komunikace, celý systém by mohl přestat být bezpečný a funkční.

6. Možnosti zřízení elektronického podpisu, jeho použitelnost, jeho výhody i nevýhody

Následující kapitola je věnována možnostem zřízení elektronického podpisu, který je určen právě pro tuto komunikaci, tedy komunikaci s úřady prostřednictvím zaručeného elektronického podpisu.

6.1 Možnosti zřízení

Zřídit si elektronický podpis není v dnešní době problém. Na internetu nebo v tisku vidíme mnoho reklam, které odkazují na zřizovatele certifikátů, respektive elektronického podpisu. Tato reklama je však zaměřena na jiné typy certifikátů, než které jsou potřeba pro komunikaci s orgány veřejné správy.

Pokud se tedy občan rozhodne, že chce použít technologii elektronického podepisování, jeho postup můžeme shrnout do následujících bodů:

- **Určení účelu elektronického podpisu,**
- **Výběr poskytovatele certifikačních služeb a certifikátu,**
- **Samotné zřízení,**
- **Použití elektronického podpisu.**

Tento postup se v mnohém neliší od postupů poskytovatelů certifikačních služeb.

I. Určení účelu elektronického podpisu

Žadatel o certifikační služby si musí určit, k jakému účelu elektronický podpis vlastně potřebuje. Pro komunikaci s veřejnou správou musí dle odst. 1 § 11 zákona č. 227/2000 Sb. použít jen zaručené elektronické podpisy založené na kvalifikovaných certifikátech od akreditovaných poskytovatelů certifikačních služeb. Pokud ovšem druhá strana komunikace nevyžaduje užití zaručeného elektronického podpisu, lze využít komerční certifikát, který nemusí být vydán kvalifikovaným poskytovatelem.

II. Výběr poskytovatele certifikačních služeb a certifikátu

Akreditace kvalifikovaných certifikačních služeb vydává Ministerstvo vnitra České republiky. V současnosti si můžeme vybrat mezi 3 poskytovateli. Liší se v nabídce poskytovaných služeb, cenou a postupem vydávání certifikátů. V následujícím přehledu (Obr. 8) jsou uvedeny nabízené služby.

První certifikační autorita, a. s.	Česká pošta, s. p.	eIdentity a. s.
<ul style="list-style-type: none">• kvalifikované certifikáty• kvalifikované systémové certifikáty• kvalifikovaná časová razítka	<ul style="list-style-type: none">• kvalifikované certifikáty• kvalifikované systémové certifikáty• kvalifikovaná časová razítka	<ul style="list-style-type: none">• kvalifikované certifikáty• kvalifikované systémové certifikáty

Obr. 8 Služby poskytovatelů certifikačních služeb

III. Samotné zřízení

Následující pasáž popisuje kroky k získání certifikátů potřebných k vytvoření elektronického podpisu.

Krok 1. Prvním krokem je vygenerování páru klíčů a žádosti o certifikát. To lze dvěma způsoby:

- **on-line** na stránkách poskytovatele
- **off-line** pomocí programu nabízeného poskytovatelem

On-line generování je výhodné, protože uživatel nemusí instalovat speciální program do počítače. Off-line metoda je určena především pro ty uživatele vlastníci omezené připojení k Internetu. Tento postup je však pomalejší než předchozí.¹⁰

V žádosti o vydání certifikátu najdeme zpravidla tyto údaje:

- jméno,
- rodné číslo,
- adresa,
- číslo občanského průkazu,
- číslo druhého dokladu totožnosti (řidičský průkaz),
- typ certifikátu, který chceme získat,

¹⁰ U poskytovatele PostSignum, resp. České pošty, je on-line generování omezeno na počítače s instalací operačního systému Windows a internetového prohlížeče Microsoft Internet Explorer.

- kód země,
- e-mailová adresa.

Krok 2. Vygenerované soubory uživatel uloží na přenosné médium (např. flash disk). Při následné návštěvě poskytovatele je nutné tento disk přeložit odpovědnému operátorovi.

Krok 3. Dalším krokem k získání certifikátu je vyplnění smlouvy o poskytování certifikačních služeb. Smlouva patří mezi dokumenty, které je třeba donést na kontaktní místo poskytovatele.

Krok 4. Následuje osobní návštěva kontaktního místa, kde žadatel předkládá výše uvedené doklady a flash disk s vygenerovaným párem klíčů. Operátor poskytovatele ověří totožnost žadatele dle 2 předložených dokladů totožnosti. Pokud vše souhlasí, dojde k uzavření smlouvy a k vystavení vyžádaného certifikátu. V rámci bezpečnosti jsou vydané certifikáty poskytovatelem zveřejněny.

Krok 5. Posledním krokem je instalace certifikátu do počítače. Instalace se liší dle softwaru poskytovatele. Pomocí souborů z flash disku je do počítače nainstalován certifikát žadatele. Ve všech případech je to však jednoduché a rychlé.

IV. Použití elektronického podpisu

Po instalaci certifikátu už nic nebrání uživateli použít elektronický podpis jako prostředek pro bezpečnou komunikaci. Dnešní základní software většiny počítačů obsahuje nástroje, které podporují připojování elektronického podpisu k dokumentům nebo souborům. V poštovním klientu uživatele (např. MS Outlook Express) je třeba nastavit v položce zabezpečení přidání podpisu ke zprávě. Po napsání zprávy uživatel zvolí příslušnou volbu přidání podpisu a zpráva je elektronicky podepsána.

6.2 Použitelnost zaručeného elektronického podpisu

Elektronický podpis lze užít téměř při každé elektronické komunikaci. Každý e-mail nebo textový dokument lze opatřit elektronickým podpisem, resp. zaručeným elektronickým podpisem. V následujícím přehledu (Obr. 9) jsou uvedeny instituce, se kterými lze komunikovat pomocí zaručeného elektronického podpisu.



Obr. 9 Subjekty užívající elektronický podpis

Následuje detailnější rozpis služeb jednotlivých institucí:

Ministerstvo práce a sociálních věcí

- Žádost o přídavek na dítě
- Žádost o sociální příplatek
- Žádost o příspěvek na bydlení
- Žádost o rodičovský příspěvek
- Hlášení změn
- Žádost o dávku pěstounské péče - příspěvek na úhradu potřeb dítěte
- Žádost o dávku pěstounské péče - odměna pěstouna
- Žádost o příspěvek na péči o dítě v zařízení pro děti vyžadující okamžitou pomoc
- Žádost o porodné
- Žádost o pohřebné

Ministerstvo vnitra

- Návrhy na zahájení správního řízení
- Návrhy na přezkoumání rozhodnutí
- Žádosti o vydání osvědčení, posudků, vyjádření, doporučení

Ministerstvo financí

- Daňové přiznání k silniční dani
- Daňové přiznání k dani z nemovitosti
- Daňové přiznání k DPH
- Daňové přiznání k dani z příjmů právnických osob
- Daňové přiznání k dani z příjmů fyzických osob
- Vyúčtování daně z příjmů fyzických osob ze závislé činnosti a z funkčních požitků
- Obecné písemnosti - žádosti, stížnosti

Česká správa sociálního zabezpečení

- Evidenční listy důchodového pojištění
- Přihlášky a odhlášky zaměstnanců k nemocenskému pojištění
- Přehled o příjmech a výdajích OSVČ

Elektronický podpis lze dále uplatnit v těchto případech

- Komunikace s krajskými, městskými či obecními úřady (e-podatelný)
- Komunikace mezi vybranými zdravotními pojišťovnami a poskytovateli zdravotní péče,
- plátcí pojistného i samotnými pojištěnci.
- podávat Oznámení pojištěnce
- Ověření pojištěnce
- Komunikace s Komisí pro cenné papíry
- Přijímání celních deklarací od celních deklarantů a komunikace v rámci celního řízení

6.3 Výhody a nevýhody elektronického podpisu

V následující tabulce č. 2 autor shrnul výhody a nevýhody elektronického podpisu vyplývající z celé práce.

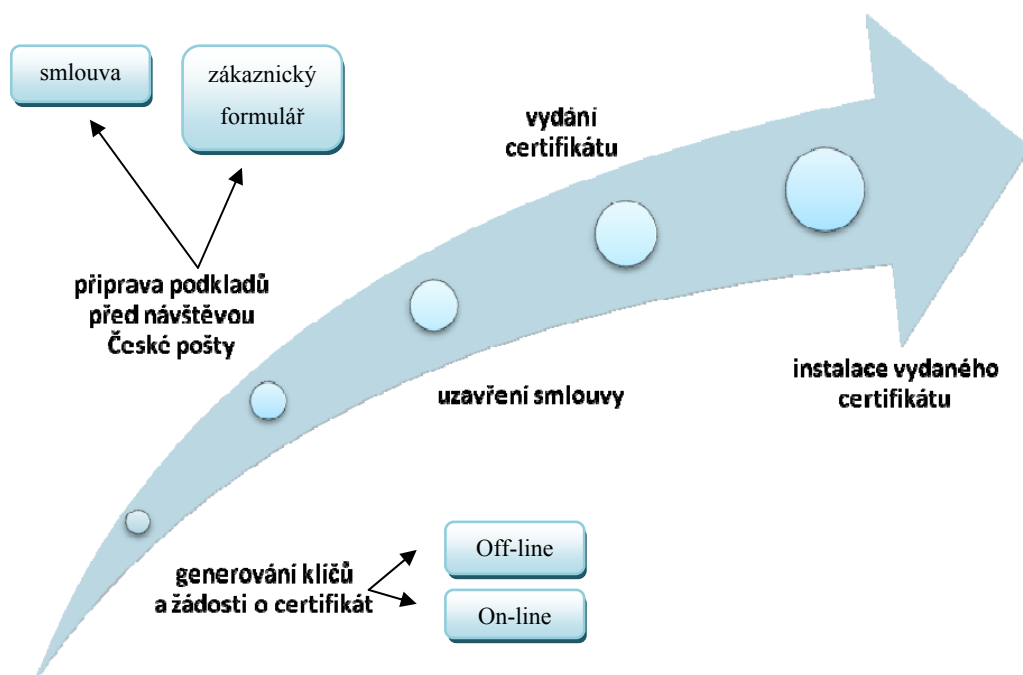
Tabulka č. 2 Výhody a nevýhody elektronického podpisu

Elektronický podpis	
výhody	nevýhody
ověření identity podepisujícího ověření integrity zprávy zaručení nepopiratelnost zprávy nenapodobitelnost podpisu rychlost komunikace s úřady snížení nákladů na státní aparát vícenásobné užití úspora nákladů za poštovné úspora lidské práce zprehlednění procesů	ztráta osobního kontaktu s úřadem finanční náročnost zavedení psychologické bariéry nízká zodpovědnost při uchování hesla

Výhody tedy výrazně převyšují nad nevýhodami. Psychologické bariéry ve sloupci „Nevýhody“ jsou uvedeny, protože stojí za stále malým rozsahem použití této technologie.

7. Získání kvalifikovaného certifikátu na pobočce České pošty

Tato kapitola uvádí přesný postup autora práce při pořizování osobního kvalifikovaného certifikátu, na jehož základě lze použít zaručený elektronický podpis. V příloženém schématu (Obr. 10) je celý postup graficky znázorněn. V závěru kapitoly autor hodnotí přístup poskytovatele k zákazníkovi.



Obr. 10 Získání kvalifikovaného osobního certifikátu na České poště

7.1 Získání kvalifikovaného certifikátu pro účely komunikace s veřejnou správou

Jako první krok k získání kvalifikovaného certifikátu je nutné si nejdříve zjistit informace u poskytovatele. V tomto případě jsou využity internetové stránky České pošty. V sekci E-slужby najdeme základní informace a nabídku služeb. Česká pošta se stala akreditovaným poskytovatelem v srpnu roku 2005 na základě rozhodnutí tehdejšího Ministerstva informatiky ČR. Informační systém, který slouží jako průvodce po celém procesu, se jmenuje PostSignum QCA.

Právě na této stránce jsou k dispozici veškeré údaje potřebné pro úspěšné podání žádosti o certifikát. Po přečtení sekce „**Základní informace**“ jsme se dozvěděli, kde můžeme kvalifikované certifikáty využít.

Poté přejdeme na následující sekci „**Přehled postupů**“. Zde musíme zadat, k jaké skupině zákazníků patříme. Jsou zde tři možnosti:

1. zástupce/zaměstnanec právnické osoby,
2. podnikající osoba (OSVČ),
3. nepodnikající fyzická osoba.

Jako „obyčejný občan“ autor zvolí možnost č. 3. Nabídne se nám kompletní karta, kde najdeme definici námi zvolené osoby žadatele. Následuje výčet postupů řazených chronologicky za sebou.

1. Vygenerování klíčů a žádosti o certifikát
2. Příprava podkladů před návštěvou České pošty
3. Uzavření smlouvy s Českou poštou
4. Vydání certifikátu
5. Instalace vydaného certifikátu

1. Vygenerování klíčů a žádosti o certifikát

Prvním krokem je vygenerování žádosti o certifikát. Jsou dvě možnosti:

- On-line generování
- Off-line generování

On-line generování přináší jistý komfort, kdy nemusíme nic instalovat do našeho počítače. Omezením v tomto případě je využití výhradně prohlížeče Internet Explorer.

Off-line generování žádosti. Zde je nutné stáhnout a nainstalovat instalační balíček podle používaného operačního systému. Soubor pro Windows XP má velikost 40 Mb. Uživatel si v této nabídce může stáhnout příručku, jak postupovat při generování klíčů. Po úspěšné instalaci nás přivítá program PostSignum Tool Plus. Tento jednoúčelový program slouží výhradně pro generování dvojice klíčů a tvorbu žádosti o certifikát. V programu

zvolíme místo na přenosném disku, kde chceme mít certifikát k dispozici. Následovalo vyplnění údajů o žadateli a zadání hesla. Toto heslo pak chrání celý certifikát. Program poté vygeneroval dvojici klíčů a žádost o certifikát.

2. Příprava podkladů před návštěvou České pošty

Druhým krokem byla příprava písemných podkladů před návštěvou pobočky České pošty. Žadatel vyplnil nabízenou objednávku certifikačních služeb (Příloha č. 3). Vše šlo velmi jednoduše v textovém editoru. Objednávka musela být vytištěna ve dvou exemplářích. Dalším dokumentem byl jeden výtisk zákaznického formuláře (Příloha č. 4). Oba dokumenty jsou podepisovány až na pobočce, kde dojde ke kontrole údajů.

3. Uzavření smlouvy s Českou poštou

Pro návštěvu pošty tedy nutné mít připraveno:

- přenosný disk s vygenerovanou žádostí a párem klíčů,
- 2 výtisky objednávky certifikačních služeb,
- 1 výtisk zákaznického formuláře,
- dva doklady osobnosti.

Na poště pověřený pracovník zkontroluje naši totožnost dle předložených dokladů. Doklady jsou pak zkopírovány na základě § 6 odst. zákona 227/2000 Sb., o elektronickém podpisu. Následně pracovník ověří všechny údaje na všech formulářích. Dojde k podepsání smlouvy. Po úspěšné kontrole zákaznického formuláře pracovník pošty zadal údaje z objednávky do systému PostSignum. Následoval tisk písemné žádosti, kde byly uvedeny údaje pro náš budoucí certifikát (více Kapitola 5).

Po kontrole údajů a podepsání žádosti je pracovníkem vydán certifikát, který je zpravidla uložen na přenosný disk žadatele. Poté pracovník pošty vytiskl protokol o předání certifikátu. Opět bylo třeba provést kontrolu údajů. To je velmi důležité, pokud by údaje nebyly dostatečně kontrolovány, bylo by pak celé elektronické podepisování ohroženo nebo by také mohl být poskytovatel sankcionován.

4. Vydání certifikátu

Po úspěšné verifikaci údajů byl na přenosný disk přenesen protokol o vydání certifikátu. Zákazník také obdrží **Žádost o vydání certifikátu** (Příloha č. 5), kde jsou

vedeny všechny údaje o certifikátu. Pracovník České pošty pak provedl základní instruktáž, jak vydaný certifikát nainstalovat. Na uvedenou e-mailovou adresu poskytovatel během příštích pár minut odešle znovu certifikát a protokol o vydání. Od této chvíle se žadatel stává vlastníkem kvalifikovaného certifikátu.

Na závěr celé návštěvy došlo k zaplacení vydání certifikátu. Kvalifikovaný certifikát stojí 190 Kč s DPH a má platnost 1 rok. Poté je nutné ho obnovit.

5. Instalace vydaného certifikátu

Po 15 minutách od vydání certifikátu byl úspěšně nainstalován na osobním počítači. Vše proběhlo pomocí nainstalovaného programu PostSignum Tool Plus, který uživatele nasměruje v instalaci. Následně byl zkušebně použit pro podepsání textového souboru. Od přečtení základních informací na stránkách České pošty až po instalaci certifikátu, uběhla téměř hodina.

7.2 Hodnocení uživatele

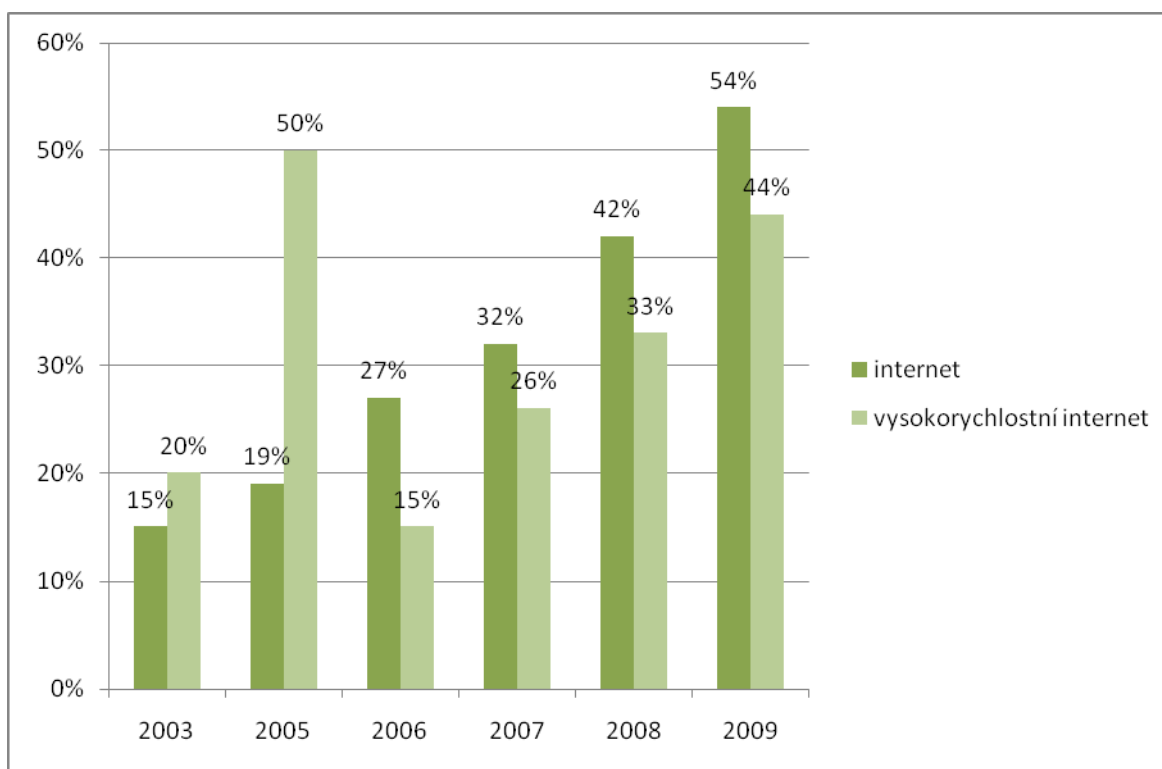
Pokud zájemce o elektronický podpis věnuje dostatečný čas informativní části na internetových stránkách České pošty, je celý proces velmi rychlý a bezproblémový. Lze také využít linku, kde najdete pomoc při technických problémech. Generování žádostí a páru klíčů lze označit za nejvíce časově náročný článek procesu. Ovšem Off-line generování bylo také uživatelsky příjemné. O pracovníci pošty, která mi vydávala certifikát, se musím vyjádřit velice kladně. Na všechny mé dotazy uměla odpovědět. Její postup práce byl systematický a bezchybný. Také její instruktáž k instalaci celého procesu byla srozumitelná a přínosná. S četbou informací na stránkách České pošty, návštěvou pobočky pošty a instalací trval celý proces přibližně 60 minut. Získání certifikátu tedy není časově ani finančně náročná operace. Porovnání s dobou, kterou běžný občan stráví na úřadech, jde o zanedbatelný čas.

8. Průzkum na téma využití elektronického podpisu v praxi

Tato kapitola obsahuje počty lidí, kteří využívají počítače, internet i certifikační služby. Z uvedených statistik lze konstatovat, že stále více lidí používá počítač s připojením na internet a stále více lidí začíná používat elektronické služby.

Jak již bylo řečeno v úvodu práce, při vyhledávání informací o počtu vydaných kvalifikovaných certifikátů nastal problém, když poskytovatelé certifikačních služeb (První certifikační autorita a eIdentity) neposkytli údaje o počtu svých vydaných kvalifikovaných certifikátů. Proto nelze uvést statistiku počtu všech aktivních certifikátů, které se v České republice používají. Ale lze uvést neaktuální údaje a údaje dostupné z výročních zpráv České pošty.

Počet lidí s připojením na internet

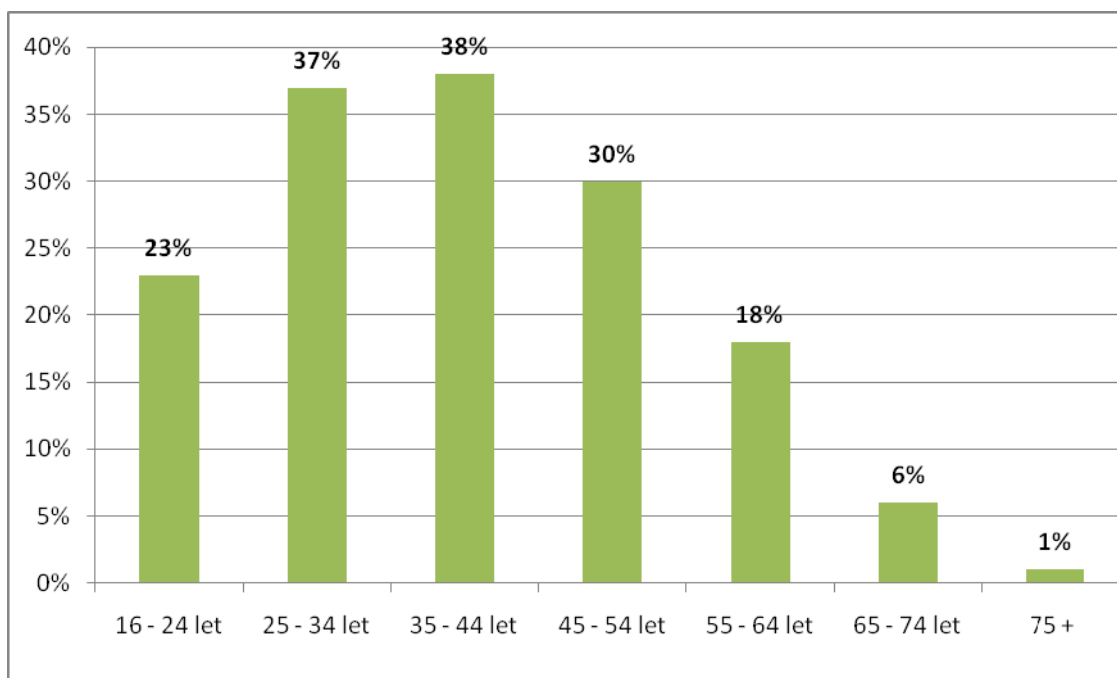


Graf 1 Počet lidí s připojením na internet

[Český statistický úřad, 2009]

Výše uvedený graf č. 1 znázorňuje růst počtu připojení k síti internet v ČR. Stoupající tendence lze jednoznačně přičíst poklesem ceny těchto služeb a tím i větší dostupnosti internetových připojení.

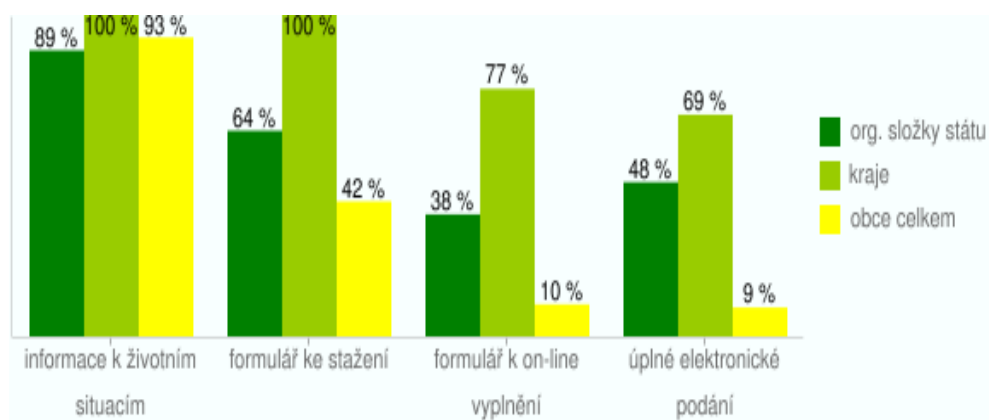
Použití internetu ke komunikaci se státní správou



Graf 2 Použití internetu ke komunikaci se státní správou

[Český statistický úřad, 2009]

Tento graf znázorňuje věkové skupiny užívající internetové připojení ve vztahu k úřadům. Nejčastější skupinou jsou uživatelé ve věku 25-44 let. Následující graf č. 3 znázorňuje míru užití jednotlivých nabídek on-line služeb. Je patrné, že uživatelé na internetových stránkách vyhledávají informace a stahují potřebné formuláře. I to lze považovat za pomoc při šetření nákladů na státní správu.



Graf 3 Graf využití služeb

[Český statistický úřad, 2009]

Množství kvalifikovaných certifikačních služeb

Poslední dostupný údaj je k 31. prosinci 2006. Tehdy fungující Ministerstvo informatiky ČR statistiky uvedlo, že všechny tři kvalifikovaní poskytovatelé certifikačních služeb společně vydali 35 050 kvalifikovaných certifikátů. Dnes se tento počet pohybuje v řádech několika statisíců vydaných kvalifikovaných certifikátů.

Česká pošta ovšem své statistiky uvádí ve svých výročních zprávách, proto jsou v níže uvedené tabulce (tab. 3) znázorněny počty kvalifikovaných certifikátů vydaných Českou poštou. Česká pošta se v roce 2009 stala lídrem v počtu vydaných kvalifikovaných certifikátů v České republice. Tyto údaje dokazují, že o kvalifikované certifikáty je stále větší zájem. Meziroční nárůst je více než 100%.

Tabulka č. 3 Počet kvalifikovaných služeb

	2007	2008	2009
komerční certifikáty	3 108	9 391	27 604
kvalifikované certifikáty	31 858	48 522	112 346
kvalifikovaná časová razítka	x	x	3 779 897

9. Závěr

Elektronický podpis je pro většinu lidí stále velkou neznámou. Jednou z příčin je fakt, že k jeho užití občany stále nic nenutí. Nemají tedy důvod, aby se o tento způsob komunikace zajímali. Další příčinou je nízká informační gramotnost občanů v České republice, která jistě v příštích letech nepřesáhne 50% hranici. Důležitou skutečností je také fakt, že ne všichni vlastní počítač s připojením k internetu. Tato skupina lidí tedy není potenciálními uživateli elektronického podpisu. Pro orgány veřejné správy, které dnes nabízejí elektronický styk s občanem, je to škoda, protože momentální světová ekonomická krize přinesla vládám většiny zemí jednu společnou věc – úsporu veřejných financí. Celý projekt elektronické veřejné správy je v pokročilém stádiu, a kdyby tedy byl využíván ve větší míře, lze předpokládat, že by to byl krok k velkým úsporám ve státním aparátu. Dnes tedy občané využívají především osobní návštěvu na úřadech a elektronický podpis je spíše záležitostí několika tisíců osob.

V následujících letech lze očekávat větší vliv Evropské unie v oblasti eGovernmentu. Na základě spolupráce s členy unie vzniká mnoho projektů, které spojují státy v jeden velký „evropský stát“. Společnou vizí je jeden velký eGovernment pro všechny členské státy. Tím by však docházelo k omezení vlivu státu na jeho chod, před čímž někteří odborníci varují. Společný výklad zákonů o elektronickém podpisu a eGovernmentu lze považovat za přípravu vybudování společné elektronické správy. Také skutečnost, že země uznávají kvalifikované certifikáty, vydané v zemích EU, tento názor podporují. Přejít na společný eGovernment by mohl přinést nesporné výhody pro všechny občany eurozóny, kteří cestují nebo žijí v jiné členské zemi. Právě zaručeným elektronickým podpisem bude moci „evropský občan“ komunikovat se svým úřadem na velkou vzdálenost. To bych považoval za největší přínos této technologie.

V dnešním světě jsou informace velmi cennou „komoditou“. Rozsah elektronické komunikace se stále zvětšuje, proto se musí dávat větší důraz na bezpečnost. Elektronický podpis sice přímo nepřináší 100% bezpečnost, ale je dostačující pro styk s veřejnou správou i běžnou komunikaci s jinými subjekty, kde je ochrana dat a informací vyžadována. Pokud bude držitel certifikátu natolik obezřetný s uchováním svého klíče a hesla, neměl by mu vzniknout problém s užitím elektronického podpisu.

Ovšem jak již bylo řečeno v této práci, elektronický podpis má také svá úskalí. Za stinnou stránku věci považují fakt, že omezí osobní komunikace člověka s člověkem.

Pokud by nastala situace, kdy člověk bude umět komunikovat pouze pomocí počítače, bude to znamenat pokrok v oblasti moderních technologií, ale schopnost člověka osobně jednat běžném osobním styku se bude snižovat.

Cílem této práce bylo shrnout celou technologii a popsat situaci v České republice. Bohužel nebylo možno dokonale popsat aktuální rozšíření elektronického podpisu v české správě, protože komplexní statistické údaje nejsou přístupné veřejnosti. Možným řešením by byl projekt většího rozsahu, který by byl mohl být více zaštitěn větší organizací, aby se dosáhlo výsledků v oblasti průzkumu veřejného mínění. Práci bych považoval za menšího průvodce po světě elektronického podpisu, protože jsou zde popsány všechny hlediska, která jsou důležitá pro občana, jakožto potenciálního uživatele elektronického podpisu.

Dle mého názoru je technologie elektronického podpisu velkým přínosem pro oblast veřejné správy. Nikdo nemá rád čekání na úřadech a stálé zařizování všech možných dokumentů. Pokud je možnost, jak se tomuto vyhnout, měl by se člověk více zajímat o elektronickou komunikaci s úřadem. V České republice však není dostatečná „reklama“ tohoto způsobu komunikace. Mnoho lidí si představuje elektronický podpis jen jako elektronického zástupce svého osobního podpisu, proto nevidí důvod, proč si jej pořizovat. Je třeba lépe informovat širší veřejnost o této problematice, aby se dosáhlo většího rozsahu použití. Elektronické podepisování, zvláště ve veřejné správě, může člověku značně ulehčit život. Kdo je schopný práce s počítačem a potřebuje častěji komunikovat se státní správou, možná by se měl nad touto technologií zamyslet a zvážit, zda se přeci jen nezapojit do světa elektronické veřejné správy a elektronického podepisování.

Seznam použité literatury

- BRATKOVÁ, Eva. (zprac.). Metody citování literatury a strukturování bibliografických záznamů podle mezinárodních norem ISO 690 a ISO 690-2 : metodický materiál pro autory vysokoškolských kvalifikačních prací [online]. Verze 2.0, aktualiz. a rozšíř. Praha : Odborná komise pro otázky elektronického zpřístupňování vysokoškolských kvalifikačních prací, Asociace knihoven vysokých škol ČR, 2008-12-22 [2010-05-03]. 60 s. (PDF). Dostupný z WWW: <<http://www.evskp.cz/SD/4c.pdf>>.
- BUDIŠ, Petr. *Elektronický podpis a jeho aplikace v praxi*. Olomouc : Anag, 2008. 157 s. ISBN 978-80-7263-465-1.
- Česká pošta. 2010a. *Výroční zpráva 2009* [online]. Dostupný z WWW ve formátu PDF: <<http://www.cpost.cz/assets/o-ceske-poste/profil/VZ-CESKA-POSTA-2009.pdf>>.
- Česká pošta. 2010b. *Výroční zpráva 2008* [online]. Dostupný z WWW ve formátu PDF: <<http://www.cpost.cz/assets/o-ceske-poste/profil/VZ-Ceska-posta-2008-CJ-.pdf>>.
- Česká pošta. 2010c. *Výroční zpráva 2007* [online]. Dostupný z WWW ve formátu PDF: <http://www.cpost.cz/assets/o-ceske-poste/profil/vz_cp_07.pdf>.
- Česká republika. *MVCR Homepage* [online]. Praha : Ministerstvo vnitra České republiky. 2008 [cit. 2010-01-30]. EGovernment. Dostupný z WWW: <<http://www.mvcr.cz/egovernment.aspx>>.
- Česko. Zákon č. 227 ze dne 29. června 2000 o elektronickém podpisu. In *Sbírka zákonů České republiky*. 2000, s. 3290-3297. Dostupný také z WWW: <<http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=3456>>. ISSN 1213-6158.

- Česko. ©2003-2010. Ministerstvo vnitra. *Portál veřejné správy České republiky* [online]. Praha : Ministerstvo vnitra České republiky, ©2003-2010 [cit. 2010-07-14]. Dostupný z WWW: <<http://portal.gov.cz>>.
- Česko. ©2010a. Ministerstvo vnitra. *Ministerstvo vnitra České republiky* [online]. Praha : Ministerstvo vnitra ČR, ©2010 [cit. 2010-07-17]. Portál veřejné správy. Dostupné z WWW: < <http://www.mvcr.cz/clanek/portal-verejne-spravy.aspx>>.
- Česko. ©2010b. Ministerstvo vnitra. *Ministerstvo vnitra České republiky* [online]. Praha : Ministerstvo vnitra ČR, ©2010 [cit. 2010-04-17]. eGON. Symbol eGovernmentu. Dostupné z WWW:<<http://www.mvcr.cz/clanek/egon-jako-symbol-egovernmentu-moderniho-pratelskeho-a-efektivniho-uradu-252052.aspx?q=Y2hudW09MQ%3d%3d>>.
- Česko. ©2010c. Ministerstvo průmyslu a obchodu. *Ministerstvo průmyslu a obchodu České republiky* [online]. Praha : Ministerstvo vnitra ČR, ©2010 [cit. 2010-06-27]. Zahraniční obchod. Dostupné z WWW: < <http://www.mpo.cz/cz/zahranicni-obchod/>>.
- Česko. ©2010d. Ministerstvo vnitra. *Ministerstvo vnitra České republiky* [online]. Praha : Ministerstvo vnitra ČR, ©2010 [cit. 2010-05-07]. Portál veřejné správy. Dostupné z WWW: < <http://www.mvcr.cz/clanek/vyhlaska-c-529-2006-sb-o-dlouhodobem-rizeni-informacnich-systemu-verejne-spravy.aspx>>.
- Česko. ©2010e. Ministerstvo vnitra. *Ministerstvo vnitra České republiky* [online]. Praha : Ministerstvo vnitra ČR, ©2010 [cit. 2010-07-02]. Archiv. Dostupné z WWW: < http://aplikace.mvcr.cz/archiv2008/micr/scripts/detail.php_id_389.html>.
- Český statistický úřad. 2009. *Využívání informačních a komunikačních technologií v domácnostech a mezi jednotlivci v roce 2009*. Praha : Český statistický úřad, 2009. Dostupný z WWW ve formátu PDF: <[http://czso.cz/csu/2009edicniplan.nsf/t/8200311384/\\$File/CSU_PublikaceICT2009.pdf](http://czso.cz/csu/2009edicniplan.nsf/t/8200311384/$File/CSU_PublikaceICT2009.pdf)>. ISBN 978-80-250-1994-8.
- DOSTÁLEK, Libor. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. 1. vyd. Brno : Computer Press, 2006. 543 s. ISBN 80-251-0828-7.

- *ISVS.CZ : informační systémy veřejné správy*. ©2001-2010. [online]. Praha : ADVICE.CZ, ©2001-2010 [cit. 2010-07-10]. Dostupný z WWW: <<http://www.isvs.cz/>>. ISSN 1802-6575.

- LIDINSKÝ, V aj. *eGovernment bezpečně*. Praha : Grada, 2008. 145 s. ISBN 978-80-247-24.

- LUHAN, Jaromír. *E-government : téma, které dnes „letí“*. *IT Systems*. 2009, roč. 11, č. 3, s. 16. ISSN 1802-002X.

- MATES, Pavel; VLADIMÍR, Smejkal. *E-Government v českém právu*. Praha : Linde, 2006. 244 s. ISBN 80-7201-614-8.

- MACKOVÁ, Alena; ŠTĚDRŮŇ, Bohumír . *Zákon o elektronických úkonech a autorizované konverzi dokumentů s komentářem : včetně souvisejících zákonů a prováděcích předpisů*. Praha : Wolters Kluwer Česká republika, 2009. 518 s. ISBN 978-80-7357-472-7.

- NEUGEBAUER, Tomáš. *Nová pravidla písemné a elektronické komunikace*. 1. vydání. Kralice na Hané : Computer Media, 2008. 136 s. ISBN 978-80-7402-011-7.

- PETERKA, Jiří. Elektronický, nebo digitální podpis?. *IT-NET*. 2000, roč. 2, č. 4, s. 31. Dostupné z WWW: <<http://www.earchiv.cz/b00/b0004001.php3>> . ISSN 1212-6780.

- PETERKA, Jiří. Česká cesta k elektronickému podpisu. *IT-NET*. 2000, roč. 2, č. 6, s. 8. Dostupné z WWW: <<http://www.earchiv.cz/b00/b0006001.php3>> . ISSN 1212-6780.

- PŘIBYL, Tomáš. *Svět elektronického podpisu*. [Česko] : AEC, [2008]. 58 s.

- RAŠEK, Luděk, MAYEROVÁ, Tereza. Bezpečnost elektronické komunikace. *IT Systems*. 2006, roč. 8, č. 11, s. 10-11. ISSN 1802-002X.

- SMOLÍK, Radek. Bezpečně s ISDS (4) : bděte nad bezpečností svého prohlížeče. *Computerworld*. 2010, roč. 21, č. 5, s. 33. ISSN 1210-9924.
- VYSTAVĚLOVÁ, Hana. Datové schránky a informační bezpečnost. *IT Systems*. 2009, roč. 11, č. 11, s. 40-41. ISSN 1802-002X.
- *Wikipedie : otevřená encyklopedie: Kryptografie* [online]. c2010 [citováno 10. 07. 2010]. Dostupné z WWW: <<http://cs.wikipedia.org/w/index.php?title=Kryptografie&oldid=5567102>>.

Seznam obrázků

Obr. 1 Úvodní stránka Portálu veřejné správy České republiky.....	15
Obr. 2 Postavička eGon	17
Obr. 3 Schéma podpisů.....	20
Obr. 4 Šifrování symetrickou šifrou	28
Obr. 5 Asymetrické šifrování.....	29
Obr. 6 Adresovaná, zašifrovaná, ale neautorizovaná zpráva.....	31
Obr. 7 Adresovaná, zašifrovaná a autorizovaná zpráva.....	32
Obr. 8 Služby poskytovatelů certifikačních služeb	46
Obr. 9 Subjekty užívající elektronický podpis.....	48
Obr. 10 Získání kvalifikovaného osobního certifikátu na České poště	51

Seznam tabulek

Tabulka č. 1 Novely zákona č. 227/2000 Sb.	37
Tabulka č. 2 Výhody a nevýhody elektronického podpisu.....	50
Tabulka č. 3 Počet kvalifikovaných služeb	57

Seznam grafů

Graf 1 Počet lidí s připojením na internet.....	55
Graf 2 Použití internetu ke komunikaci se státní správou	56
Graf 3 Graf využití služeb	56

Příloha 1

DESATERO BEZPEČNOSTI V INFORMAČNÍM SYSTÉMU DATOVÝCH SCHRÁNEK

- Bezpečný přístup k datové schránce**
Ke vstupu do datové schránky je nutné přihlašovací jméno a heslo. První poštou doručené heslo si musíte změnit. Nové heslo musí mít nejméně 8 znaků a mělo by obsahovat kombinaci malých a velkých písmen, speciálních znaků (diakritika) a číslic. Přihlašování pod přístupovým jménem a heslem je pouze základní postup. Doporučujeme Vám rozšířit si zabezpečení přístupu prostřednictvím certifikátu zaručujícím bezpečnost používání datové schránky.
- Aktualizujte operační systém a bezpečnostní software**
Pamatujte, že bezpečný je pouze legální operační systém a bezpečnostní software, který je pravidelně aktualizován. Ideální je forma automatických aktualizací, která nejlépe chrání Váš počítač. Naopak pokud nemáte pravidelně aktualizovaný operační systém a bezpečnostní software, stává se Váš počítač snadným cílem útoku. Zejména Váš internetový prohlížeč, jakožto hlavní brána Vašeho přístupu do datové schránky, nesmí mít žádné tzv. bezpečnostní díry, proto jej udržujte stále aktualizovaný.
- K datové schránce přistupujte stejně obezřetně jako k internetovému účtu v bance**
Celková bezpečnost datové schránky je dána i Vaším chováním. Rozhodně je namístě při přístupu do datové schránky vypnout všechny tzv. systémy výměny rychlých zpráv, jakými jsou např. programy Skype či ICQ apod., neboť jejich prostřednictvím stahujete obsah i z neproverěných stránek, které mohou Váš počítač poškodit. Při přístupu do datové schránky proto ukončíte všechny ostatní aplikace (připojené k internetovým serverům), zavřete internetový prohlížeč, znovu ho otevřete a teprve poté se přihlaste do Vaší datové schránky.
- Používejte kvalitní antivirovou ochranu**
Pro ochranu před stále novými počítačovými viry je nutné mít legální, kvalitní a pravidelně aktualizovaný antivirový program. Před přístupem do datové schránky zkontrolujte, že máte antivirový software nainstalovaný ve Vašem počítači, že je zapnutý a že obsahuje nejaktuálnější sadu virových definic. Pokud je paměťově rezidentní antivirová ochrana počítače vypnuta, je okamžitá ochrana nulová. Nemá-li antivirus aktualizován, stává se Váš počítač snadným terčem virového útoku.
- Používejte obousměrný osobní firewall**
Firewall je bezpečnostní software, který kontroluje komunikaci Vašeho počítače s ostatními počítači. Některé firewally mohou kontrolovat pouze provoz směrem do Vašeho počítače, jiné kontrolují i provoz, který z Vašeho počítače odchází. Pouze obousměrné firewally ochrání citlivé informace, které prochází přes datové schránky. Při potížích vymažte všechna pravidla a postupným připojováním se k používaným internetovým serverům vytvořte pravidla nová. Kvalitní osobní firewally to umí udělat automaticky, aniž by si vyžadovaly Vaše zadání.
- Nepracujte a neprohlížejte internetové stránky pod účtem administrátora**
Nikdy nepracujte a nepoužívejte účet administrátora k prohlížení internetových stránek. Při napadení Vašeho počítače by totiž mohlo dojít ke změně jakéhokoliv jeho nastavení a ke kompletnímu převzetí správy systému Vaší datové schránky mnohem snadněji. Účet administrátora by měl sloužit zejména pro správu operačního systému, jako např. pro instalaci nových aplikací apod.
- Zálohujte svá důležitá data**
Pravidelně zálohujte data uložená ve Vašem počítači. Ztráta osobních dat, včetně dat uložených v systému datových schránek, může být nevratná. Pokud v rámci systému nepoužíváte službu dlouhodobého uchovávání, budou data ve Vaší datové schránce ze zákona smazána po 90 dnech od doručení.
- Používejte bezpečné bezdrátové připojení**
Bezdrátové sítě se z hlediska bezpečnosti rozdělují na zabezpečené (chráněné hesly, certifikáty nebo klíči) a nezabezpečené (ze se k nim připojí např. v kavárně). Při připojení pomocí nezabezpečené bezdrátové sítě existuje nebezpečí odposlechu komunikace. Z toho důvodu je užitečné změnit konfiguraci takové sítě na zabezpečenou. I když Informační systém datových schránek komunikuje šifrovaně, je v každém případě vhodné přihlašovat se pomocí zabezpečené bezdrátové sítě.
- Nedůvěřujte neověřeným zprávám, může se jednat o podvodné zprávy**
Informační systém datových schránek komunikuje pouze bezpečným způsobem. Nikdy nepožaduje vložení přihlašovacích, osobních či jiných citlivých údajů do datové schránky odesílatele. Pokud obdržíte datovou zprávu s požadavkem na zadání Vašich osobních dat, jedná se o podvodnou zprávu. Při nastavení notifikace zpráv elektronickou poštou či přes SMS Vám nikdy nebude doručena zpráva obsahující internetový odkaz, tlačítko nebo obrázek, na který lze kliknout. Na takové zprávy v žádném případě nereagujte, informujte o nich prosím pracoviště infolinky a poté je smažte.
- Instalujte a užívejte pouze legální software z prověřených zdrojů**
Riziko plyne i z instalace neznámých aplikací, jejichž původ nebo skutečné funkce nelze prověřit. Nezáleží na popisu těchto aplikací, ale na ověřitelnosti zdroje a jeho zabezpečení. Existuje totiž řada aplikací, jejichž účelem je implementovat do počítače software, s jehož pomocí mohou být zcizena a následně zneužita Vaše osobní data či Vaše identita v počítači uložená. Základním principem zachování bezpečnosti Vašeho počítače je proto bezvýhradně používání pouze bezpečných a legálních aplikací.

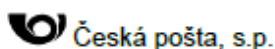
Příloha 2

Seznam legislativních dokumentů

- Doporučení UNCITRAL, týkající se právní závaznosti elektronických údajů (1985),
- Vzorový zákon UNCITRAL o elektronickém obchodu (1996),
- Vzorový zákon o elektronickém podpisu (2001),
- Zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech,
- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů,
- Zákon č. 227/2000 Sb., o elektronickém podpisu,
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy,
- Zákonem č. 517/2002 Sb., o některých opatřeních v soustavě ústředních orgánů státní správy,
- Zákon č. 440/2004 Sb. změna zákona o elektronickém podpisu,
- Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů,
- Vyhláška č. 496/2004 Sb. k elektronickým podatelním,
- Zákon č. 501/2004 Sb., kterým se mění některé zákony v souvislosti s přijetím správního řádu,
- Zákon č. 635/2004 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o správních poplatcích,
- Zákon č. 444/2005 Sb., o územních finančních orgánech,
- Zákon č. 81/2006 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů,
- Vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb,
- Zákon č. 110/2007 Sb., o některých opatřeních v soustavě ústředních orgánů státní správy,
- Zákon č. 124/2008 Sb., o Rejstříku trestů,
190/2009 Sb., o změně zákona o archivnictví a spisové službě a změna dalších zákonů,

- Zákon 223/2009 Sb. o volném pohybu služeb,
- Zákon č. 227/2009 Sb., změna zákonů v souvis. s přijetím zákona o základních registrech,
- Zákon č. 281/2009 Sb., kterým se mění některé zákony v souvislosti s přijetím daňového řádu,
- Zákon č. 101/2010 Sb., změna zákona o elektronickém podpisu a změny dalších zákonů.

Příloha 3



SMLOUVA O POSKYTOVÁNÍ CERTIFIKAČNÍCH SLUŽEB

Číslo smlouvy: _____

1. Smluvní strany

Poskytovatel

Česká pošta, s.p.

zastoupená:

se sídlem

Politických vězňů 909/4, 225 99 Praha 1

IČ:

47114983

DIČ: CZ47114983

zapsaná v

obchodním rejstříku, vedeném u Městského soudu v Praze, sp. zn. A 7565

Bankovní spojení

ČSOB, a.s., č.ú.133406370/0300

Zákazník

Jméno a příjmení _____

Adresa trvalého
bydliště _____

2. Trvání smlouvy

Tato smlouva se uzavírá na

dobu neurčitou

dobu určitou

od _____ do _____

3. Rozsah poskytovaných služeb

Zákazník má nárok využívat následující služby Poskytovatele. Poskytnutí služby je podmíněno dodáním zákaznického formuláře, v němž jsou specifikovány parametry služby.

Certifikáty vydávané kvalifikovanou certifikační autoritou PostSignum QCA:

- kvalifikované osobní certifikáty
- kvalifikované systémové certifikáty

Certifikáty vydávané komerční certifikační autoritou PostSignum VCA:

- komerční osobní certifikáty
- komerční serverové certifikáty
- šifrovací certifikáty skupin osob

4. Obecné parametry poskytovaných služeb

4.1 V případě, že nehodláte ve smyslu čl.7, odst.2b, Všeobecných obchodních podmínek, udělit poskytovateli svůj souhlas se zpracováním vašich osobních údajů za účelem marketingu či propagace produktů a služeb poskytovatele, zaškrtněte →

5. Společná a závěrečná ustanovení

5.1 Dne 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.

5.2 Povinnosti a odpovědnosti zákazníka i poskytovatele jsou uvedeny v těchto dokumentech: Všeobecné obchodní podmínky elektronických služeb České pošty, Certifikační politiky. Aktuální verze dokumentů jsou k dispozici na webových stránkách www.postsignum.cz. Podpisem této smlouvy zákazník prohlašuje, že se seznámil s obsahem těchto dokumentů.

5.3 Cena za poskytované služby je uvedena v Ceníku služeb, jehož aktuální verze je umístěna na webových stránkách www.postsignum.cz.

5.4 Změny v dokumentech uvedených v odstavcích 5.2 a 5.3 nepodléhají udělení písemného souhlasu ze strany zákazníka. Plánované změny těchto dokumentů budou v předstihu zveřejněny na stránkách www.postsignum.cz.

5.5 Způsob reklamace poskytovaných služeb je popsán v samostatném Reklamačním řádu, jehož aktuální verze je k dispozici na webových stránkách www.postsignum.cz.

5.6 Spory, které z tohoto vztahu vzniknou, se řeší u věcně a místně příslušného soudu.

5.7 Tato smlouva je vyhotovena ve dvou stejnopisech. Každá smluvní strana obdrží jedno vyhotovení smlouvy.

5.8 Akceptací této smlouvy ze strany poskytovatele dojde k uzavření smlouvy o poskytování služeb certifikační autority PostSignum.

6. Podpisy smluvních stran

Za Poskytovatele

Místo

Datum

Jméno a příjmení

Podpis

Za Zákazníka

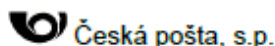
Místo

Datum

Jméno a příjmení

Podpis

Příloha 4



Česká pošta, s.p.

Příloha č.1 smlouvy o poskytování certifikačních služeb

Číslo smlouvy: _____

Údaje pro vydávání certifikátů

Osobní údaje zákazníka

Jméno a příjmení:	
Rodné číslo (občané ČR):	
Datum narození (cizinci bez rodného čísla):	

Zasiílat zákazníkovi automatické e-maily s upozorněním na končící platnost certifikátů.

Údaje o certifikátu

Žádám o vydávání kvalifikovaných certifikátů s těmito údaji:

Povinné položky:		Pravidlo zavedeno: <input type="checkbox"/>
Certifikační politika	Kvalifikované certifikáty osob	
CN (jméno a příjmení, tituly)		
E-mailová adresa		
Nepovinné položky:		
L (adresa trvalého bydliště žadatele) ¹		
Jiné jméno (údaj určený zákazníkem) ²		

Zveřejnit vydaný certifikát na webových stránkách a adresářovém serveru (LDAP) certifikační autority.

Vložit Identifikátor klienta MPSV (IK MPSV) do certifikátu.

Žádám o vydávání komerčních certifikátů s těmito údaji:

Povinné položky:		Pravidlo zavedeno: <input type="checkbox"/>
Certifikační politika	Komerční certifikáty osob	
CN (jméno a příjmení, tituly)		
E-mailová adresa		
Nepovinné položky:		
L (adresa trvalého bydliště žadatele) ¹		
Jiné jméno (údaj určený zákazníkem) ²		

Zveřejnit vydaný certifikát na webových stránkách a adresářovém serveru (LDAP) certifikační autority.

V případě rozporu údajů CN a L s údaji v předložených dokladech se do certifikátu vloží údaje z dokladů.

Legenda:

¹ Adresu zadávejte ve tvaru „Ulice číslo PSČ Obec Stát“.

² Není předepsán obsah údaje Jiné jméno. Zákazník může uvést jakýkoliv text podle vlastního uvážení.

Podpisy smluvních stran:

Za zákazníka

Za poskytovatele

Příloha 5

Číslo smlouvy: 121011-200100

Žádost o vydání certifikátu

Údaje o zákazníkovi:

Jméno:	Čeněk Kudrna
Rodné číslo:	8703260676

Údaje o žadateli o certifikát:

Jméno:	Čeněk Kudrna
Rodné číslo:	8703260676
Typ a číslo osobního dokladu:	Občanský průkaz 112821728
Typ a číslo sekundárního dokladu:	Řidičský průkaz EE 066024

Údaje o certifikátu:

V souladu se smlouvou o poskytování certifikačních služeb žádám o vydání certifikátu na základě následujících údajů.

Základní údaje

Certifikační politika:	Kvalifikované osobní certifikáty
Sleva:	Bez slevy

Předmět certifikátu

Položka předmětu	Údaj z el. žádosti o certifikát	Údaj požadovaný zákazníkem
Kód země (C):	CZ	CZ
Lokalita (L):		Nová Pražská 1646 256 01 Benešov Česko
Identifikátor osoby (OU):		P235168
Jméno certifikátu (CN):	Čeněk Kudrna	Čeněk Kudrna
Identifikátor osoby (serialNumber):		P235168

Rozšíření certifikátu

Položka předmětu	Údaj z el. žádosti o certifikát	Údaj požadovaný zákazníkem
E-mailová adresa 1:	kudrnacenek@seznam.cz	kudrnacenek@seznam.cz
E-mailová adresa 2:		
E-mailová adresa 3:		
Identifikátor MPSV:		Ano
Jiné jméno:		

Ostatní údaje

Jméno souboru se žádostí o certifikát:	cert_sign_Čeněk Kudrna_1277450023953.req
Požadované heslo pro zneplatnění:	c5++.eR*C7
Velikost veřejného klíče:	2048 bitů
SHA-1 otisk veřejného klíče:	F692 B2A4 CDC0 8FCE EEC0 8C11 35A6 0A3C 597F 7A27
SHA-1 otisk souboru se žádostí o certifikát:	265A 4C5B E218 1F25 1C04 D966 475C 4F07 4E8D 6EBA

Důkladně zkontrolujte údaje ve sloupci 'Údaj požadovaný zákazníkem'. Na pozdější reklamace nebude brán zřetel.

Práva a povinnosti žadatele o certifikát i poskytovatele jsou uvedeny v těchto dokumentech: Všeobecné obchodní podmínky vybraných elektronických služeb České pošty, Certifikační politiky. Aktuální verze dokumentů jsou k dispozici na webových stránkách www.postsignum.cz. Podpisem této žádosti žadatel o certifikát prohlašuje, že se seznámil s obsahem těchto dokumentů a že s nimi souhlasí.

25.6.2010

Datum

Podpis žadatele o certifikát

