Vysoká škola ekonomická v Praze

Fakulta managementu v Jindřichově Hradci

B a k a l á ř s k á p r á c e

Pavel Buryánek

2008

Vysoká škola ekonomická v Praze

Fakulta managementu v Jindřichově Hradci

Katedra managementu informací

Elektronická komunikace s veřejnou sférou

Autor práce: Pavel Buryánek
Vedoucí práce: Ing. Pavel Pokorný

Jindřichův Hradec 2008

VŠE

FAKULTA MANAGEMENTU

Vysoká škola ekonomická v Praze
Jarošovská 1117/II, 377 01 Jindřichův Hradec

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

pro akademický rok 2006/2007

Název práce:	**Elektronická komunikace s veřejnou sférou.**
Zadání práce:	Veřejná sféra nabízí stále více možností elektronické komunikace na různé úrovni, stav se mění rok od roku. Práce zhodnotí současný stav, ukáže stávající možnosti jak teoreticky, tak prakticky, zároveň i upozorní na možnosti zneužití. Součástí práce budou vytvořené modelové studie komunikace.
Jméno studenta:	Pavel Buryánek
Ročník:	2.
Obor:	MANAGEMENT
Vedoucí práce:	Ing. Pavel Pokorný
Katedra:	Katedra managementu informací
Termín zadání:	23.6.2006
Termín odevzdání:	Dle vyhlášky o průběhu státních závěrečných zkoušek v ak. roce 2006/2007

V Jindřichově Hradci 23.6.2006

Ing. Vladimír Přibyl
proděkan pro pedagogickou činnost

tel.: 384 417 200 fax: 384 417 277 bank. spoj. ČSOB a. s. J. Hradec
IČ: CZ61384399 č. ú. 170922147/0300

Prohlášení

Prohlašuji, že jsem bakalářskou práci na téma **Elektronická komunikace s veřejnou sférou** vypracoval samostatně. Použitou literaturu a podkladové materiály uvádím v přiloženém seznamu literatury.

Podpis autora:

Anotace

Elektronická komunikace s veřejnou sférou

Práce popisuje vývoj v posledních devíti letech a hodnotí současný stav elektronické komunikace s veřejnou sférou, ukazuje stávající možnosti jak teoreticky, tak prakticky, včetně možností jejího zabezpečení. Součástí práce jsou vytvořené modelové studie komunikace.

Electronic Communication with the Public Sphere

The work describes development in last nine years and evaluates current situation of electronic communication with the public sphere, shows current possibilities both theoretically and practically, including possibilities of its security. The work includes created model situations of communication.

Poděkování

Chtěl bych poděkovat panu **Ing. Pavlu Pokornému,** z Vysoké školy ekonomické v Praze, Fakulty managementu v Jindřichově Hradci za cenné rady, náměty, inspiraci a trpělivost při vedení mé bakalářské práce.

Pavel Buryánek

Obsah

Úvod

Veřejná sféra nabízí stále více možností elektronické komunikace na různé úrovni. V této práci se zabývám vývojem elektronické komunikace s veřejnou sférou v posledních devíti letech a pojmem eGovernment. Dalším objektem mého zájmu je mapování současných možností elektronické komunikace mezi občany a orgány veřejné správy a mezi těmito orgány navzájem, včetně určení možností zabezpečení. Součástí práce jsou také modelové situace, které slouží jako praktická ukázka využití internetu ke komunikaci nebo vyřízení povinností souvisejících s veřejnou sférou.

S rozvojem informačních technologií a zvyšující se počítačovou gramotností obyvatel se hlavně v posledních letech rozšiřují možnosti zjednodušení komunikace s orgány veřejné sféry. Tímto zjednodušením se rozumí možnost komunikovat s veřejnou sférou elektronicky. Jednou z podmínek, aby mohla taková elektronická komunikace probíhat, je ale dostatečná úprava právního rámce. Především za posledních devět let vyšla z Parlamentu ČR řada zákonů, dotýkajících se elektronické komunikace. Jedny z prvních byly například Zákon o svobodném přístupu k informacím, který mimo jiné upravil poskytování informací prostřednictvím elektronické pošty nebo Zákon o elektronickém podpisu.

Řada těchto legislativních úprav, měla počátek na již bývalém Ministerstvu informatiky ČR, které vzniklo v roce 2003 a mělo za úkol pokročit v rozvoji elektronizace státu. Kromě těchto legislativních úprav se ministerstvo podílelo i na řadě projektů. Nejznámějším z nich je asi Portál veřejné správy, který slouží jako zdroj informací a rozcestník, vedoucí na stránky státních úřadů a ministerstev.

V poslední době se hodně mluví o pojmu eGovernment. Pod tímto označením se skrývá právě proces elektronizace veřejné správy. S daným pojmem je spojena řada projektů veřejné správy. Asi největším, co se týče plošného dopadu, je eGon, projekt Ministerstva vnitra ČR, který byl představen v minulém roce na konferenci ISSS, Internet ve státní správě a samosprávě. Skládá se z několika částí, z nichž pravděpodobně nejvýznamnější je v současnosti Czech POINT. Dalším zajímavým projektem je Virtuos, který má zatím pouze regionální význam, ale do budoucna má ambice spolupracovat se zmiňovaných Czech Pointem a zahrnovat obce a města z celé České republiky.

V ČR každoročně probíhá i řada soutěží, které vybírají aktuální nejlepší projekty týkající se elektronizace veřejné sféry. Jde například o Egovernment The Best, soutěž vyhlašovanou

magazínem Egovernment, která již druhým rokem vybírá nejlepší projekty na základě kriterií převzatých z European eGovernment Awards. Další obdobnou soutěží je Zlatý erb, soutěž jejíž výsledky jsou každoročně vyhlašovány na konferenci ISSS. Hodnotí se zde nejlepší webové stránky a elektronické služby měst, obcí a krajů. V této práci jsem se rozhodl soustředit na prvně jmenovanou a na popsání vybrané trojice nejlepších projektů.

Elektronickou komunikaci je třeba také zabezpečit. Toto zabezpečení musí probíhat jednak přímo na straně uživatele, to znamená zabezpečení komunikujících počítačů, a dále je třeba zabezpečit i předávanou informaci, případně informační kanál. Z tohoto důvodu se v práci věnuji i této otázce, jmenovitě symetrickému a asymetrickému šifrování, certifikaci a elektronickému podpisu.

Jako součást práce jsem rozhodl prakticky vyzkoušet některé možnosti, které v současnosti eGovernment nabízí. Jedná se o elektronické podání daňového přiznání k silniční dani prostřednictvím stránek ministerstva financí, vznesení dotazu na městský úřad prostřednictvím e-mailu a elektronické podání přihlášky ke studiu na vysoké škole, konkrétně na Vysoké škole ekonomické v Praze.

1 Vývoj komunikace veřejnou sférou

1.1 Státní informační politika ČR

Rozšíření možností komunikace spojené s nástupem masového využívání internetu znamenalo i rozvoj možností komunikace mezi orgány veřejné správy a občany. Rok 1999 znamenal v této oblasti zásadní zlom. Orgány veřejné správy si totiž začaly uvědomovat potřebu vytvoření korektního prostředí pro fungování budoucí formy společnosti, informační společnosti. Došlo tak k vypracování dokumentu nazvaného Státní informační politika. Tato první celostátní koncepce si vzala mimo jiné za cíl dosáhnout informační gramotností všech občanů, realizovat právo občana na přímý přístup k informacím, vybudovat komunikační infrastrukturu pro veřejnou správu nebo zajistit stabilitu a bezpečnost informační společnosti.

1.2 Zákon o svobodném přístupu k informacím

Základním kamenem úpravy elektronické komunikace s veřejnou správou je Zákon o svobodném přístupu k informacím[1], který mimo jiné umožnil vyřizování žádostí o informace prostřednictvím elektronické pošty. Tento zákon platí v České republice již skoro devět, upravuje podmínky svobodného přístupu k informacím a stanovuje základní podmínky jejich poskytování. Ukládá státním orgánům, územním samosprávným celkům a veřejným institucím povinnost nezatajovat informace vztahující se k jejich působnosti. Právo tyto informace vyžadovat má jakákoli fyzická i právnická osoba. Úředníkům je zároveň stanovena povinnost odpovědět do 15 dnů na jakoukoli žádost nebo dotaz. V zákoně jsou mimo jiné upraveny i náležitosti těchto žádostí, způsob poskytování požadovaných informací včetně postupu při podávání a vyřizování písemných žádostí. Ve znění dalších novel byly odstraněny některé překážky, které znesnadňovaly využívání těchto služeb. Šlo například o zrušení možnosti úřadů libovolně či svévolně požadovat úhradu za vyhledávání informací, ale možnost žádat pouze o materiálové náklady, tzn. poštovné, cena kopie apod. Dále je podle novely určena povinnost orgánu poskytovat informace v takovém formátu, o jaký zájemce požádal a zároveň je stanovena preference poskytování informací elektronickou cestou.

[1] zákon č. 106/1999 Sb. novelizovaný zákonem č. 61/2006 Sb.

1.3 Zákon o elektronickém podpisu

Na Zákon o svobodném přístupu k informacím navázal v roce 2000 Zákon o elektronickém podpisu[2]. Ten upravuje používání elektronického podpisu, poskytování souvisejících služeb, kontrolu stanovených povinností a sankce. Dále obecně upravuje údaje v elektronické podobě, které jsou připojené k datové zprávě a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě. Zákon definuje například soulad s originálem; povinnosti podepisující osoby a poskytovatele certifikačních služeb; odpovědnost za škodu; způsob akreditace a dozoru; podmínky udělení akreditace a další. *„Bohužel však trvalo další téměř rok a půl, než byl vydán prováděcí právní předpis k tomuto zákonu, jenž tuto funkci elektronického podpisu fakticky umožnil realizovat v praxi.“*[3]

1.4 Úřad pro veřejné informační systémy

V roce 2000 vznikl Úřad pro veřejné informační systémy a byla schválena úprava, která měla umožnit koordinaci informačních systémů ve veřejné správě tak, aby spolu mohly tyto systémy vzájemně komunikovat a vyměňovat si data. Bohužel ale zůstalo pouze u záměru a tato úprava nepřinesla zamýšlené účinky. V roce 2000 došlo také ke vzniku Úřadu na ochranu osobních údajů, v jehož kompetenci je dohlížení nad zpracováváním osobních údajů.

1.5 Státní informační a komunikační politika

Další významná změna se udála až o tři roky později, kdy zanikl Úřad pro veřejné informační systémy a byl nahrazen nově zřízeným ministerstvem informatiky. Tomu se za dobu své existence[4] podařilo připravit a prosadit několik novel právních předpisů, jako například novelu zákona o elektronickém podpisu. Vznik ministerstva informatiky ale znamenal také významný odklon od původních ambiciózních strategických dokumentů přijatých v roce 1999. Ty byly totiž přehodnoceny a vše vyústilo ve schválení Státní informační a komunikační politiky, známé též pod názvem e-Česko. Jako členská země EU se Česká republika následně přihlásila i k aktualizovanému evropskému akčnímu plánu „eEurope 2005: Informační společnost pro všechny“. Bohužel je ale nutno říct, že řada cílů stanovených ve Státní informační a komunikační politice nebyla ve svém termínu do roku 2006 splněna. Jednalo se například o *„cíl připravit legislativní úpravu pravidel pro výměnu*

[2] zákon č. 227/2000 Sb.
[3] Štědroň, B.: *Úvod do eGovernmentu*, Praha: Úřad vlády České republiky, 2007, str. 20
[4] Ministerstvo informatiky ukončilo svou činnost jako samostatný resort dne 31. května 2007

dat mezi orgány veřejné správy a postavení základních registrů veřejné správy"[5] nebo o cíl co největší eliminace povinnosti občana předkládat orgánům veřejné správy dokumenty v listinné podobě, pokud mají orgány možnost poskytovat si tyto dokumenty elektronicky mezi sebou.

Je nutné ještě poznamenat, že agendy bývalého ministerstva informatiky byly převedeny na ministerstvo vnitra, ministerstvo průmyslu a obchodu a ministerstvo pro místní rozvoj.

[5] Štědroň, B.: *Úvod do eGovernmentu*, Praha: Úřad vlády České republiky, 2007, str. 21

2 eGovernment

2.1 Úvod

V posledních letech probíhá proces elektronizace veřejné správy, tzv. eGovernment (ISVS[6]). Jeho cílem je zrychlení, zvýšení spolehlivosti a snížení nákladů při poskytování služeb široké veřejnosti a zajištění větší otevřenosti orgánů veřejné správy ve vztahu k občanům. Konkrétním úspěšným nasazením eGovernmentu v praxi je například projekt Czech POINT. Je to projekt ministerstva vnitra, jehož cílem je umožnit občanům získat všechny potřebné dokumenty, vydávané veřejnou správou, pouze na jednom místě.

2.2 Související pojmy

E-government – „*série procesů vedoucích k výkonu státní správy a uplatňování občanských práv a povinností fyzických i právnických osob, realizovaných elektronickými prostředky.“*[7]

G2B – je to zkratka, která vznikla z anglického výrazu Government to Business a týká se obchodních vztahů a komunikace mezi státní správou a obchodníkem. Koncept G2B je součástí eGovernmentu a spadá do něj např. zadávání veřejných zakázek, informace o grantech apod.

B2G – pojem je využíván zejména v oblasti e-commerce pro označení obchodního vztahu a komunikace se státní správou. Do tohoto segmentu patří nabídka produktů institucím státní správy včetně komunikace s těmito subjekty. Jedním z příkladů může být možnost podávat daňová přiznání s využitím elektronického podpisu.

E-commerce – relativně široký pojem, který je používán k označení obchodních transakcí realizovaných prostřednictvím internetu a dalších elektronických prostředků. Často se ještě rozlišuje podle cílově skupiny na B2B e-commerce, která je zaměřená na obchodníky, a B2C e-commerce s orientací na konečné zákazníky.

[6] Informační systémy veřejné správy
[7] Štědroň, B.: *Úvod do eGovernmentu*, Praha: Úřad vlády České republiky, 2007, str. 9

C2G – je to zkratka, která vznikla z anglického výrazu Citizen to Government. Týká se vztahů mezi občanem a správou a je podmnožinou eGovernmentu. Jeho nejčastěji používaným příkladem je podávání daňových přiznání elektronickou formou s využitím elektronického podpisu.

G2C – jedná se o přesmyčku předcházející zkratky. Její základ je v anglickém výrazu Government to Citizen. Touto zkratkou se *„označují vztahy a komunikace mezi státní správou a běžnými občany.“*[8]

G2G – další pojem spadající do oblasti eGovernmentu. Je to zkratka pocházející z anglického termínu Government to Government a označuje se jí vzájemná komunikace mezi různými orgány veřejné moci.

Datové schránky – v současné době připravovaný projekt. Z důvodu stále se zvyšujících nákladů na poštovné, má stát v plánu zasílat formou G2B vše namísto dopisy do webové datové schránky, kterou by si museli podnikající osoby povinně založit. Pro občany by pak mělo být toto zřízení dobrovolné.

IP telefonie – přenos hlasu prostřednictvím datových sítí. Vlastní hlasová informace je přenášena prostřednictvím komunikačních sítí založených na protokolu IP. Na principu IP telefonie fungují například Instant Messengery.

Instant messengery – programy, které umožňují chatování mezi dvěma nebo více lidmi. Jejich prostřednictvím lze také poslat soubor, SMS nebo i telefonovat po internetu. Jako příklad lze uvést prakticky nejrozšířenější instant messengery, ICQ a Skype.

ICQ – pod tímto názvem se skrývá nejrozšířenější a nejpoužívanější klient umožňující zejména odesílání krátkých zpráv, sms, přenášení dat a hlasovou komunikaci včetně podpory webových kamer. Funguje velice jednoduše, každému uživateli je při registraci přiděleno jeho číslo, tzv. UIN. Toto číslo funguje v podstatě jako telefonní číslo a na jeho základě se pak do programu přihlašuje a nebo hledají subjekty, se kterými chceme komunikovat.

[8] G2C, http://www.adaptic.cz/znalosti/slovnicek/g2c.htm, cit. [13. 4. 2008] online

Skype – program, který je využíván především jako prostředek bezplatného telefonického spojení mezi uživateli internetu. Jeho prostřednictvím lze telefonovat i do pevných a mobilní sítí, a to jak domácích tak zahraničních. Tyto hovory jsou ale již zpoplatněny. Skype nabízí i řadu doprovodných funkcí. Stejně jako u ICQ lze jeho prostřednictvím posílat krátké zprávy nebo doplnit hovory o přenos obrazu prostřednictvím webových kamer. Pro využívání je třeba registrace, při které si uživatel zvolí mimo jiné svůj tzv. nick, podle kterého je následně rozpoznatelný.

2.3 Překážky rozvoje v letech 1999–2006

Dle Bohumíra Štědroně[9] Česká republika v zavádění eGovenmentu v letech 1999–2006 značně zaostala oproti svému potenciálu, který byl vytvořen především vznikem ministerstva informatiky. Nejzásadnější problémem se v oblasti budování eGovernmentu jevila, a bohužel dosud jeví, neexistence legislativní úpravy, která by umožnila patřičný rozvoj služeb poskytovaných online. Neexistuje totiž jednotný právní předpis, který by upravoval jednotná pravidla pro sdílení dat při výkonu veřejné moci, *„a to ani pro poskytování informací z informačních systémů veřejné správy pro potřeby výkonu veřejné moci jinými orgány veřejné moci, ani pro sjednocování údajů vedených v informačních systémech typu registrů.“*[10] Problém absence jednotných pravidel byl zapříčiněn i tím, že se ministerstvo informatiky zaměřilo především na zpřístupnění veřejných agend a dalo si za cíl především zpřístupnění alespoň 25 % agend veřejné správy online do roku 2006. Je ale nutno poznamenat, že ani v tomto ohledu nebyla snaha ministerstva korunována úspěchem. Z cca 550 druhů podání v jednotlivých agendách na úrovni obcí a krajů bylo pouze 10 možno vyřídit čistě elektronicky. U ostatních existovali překážky a to buď legislativního charakteru a nebo věcného charakteru.

Ministerstvo při této snaze podcenilo back office[11], takže dochází stále k situacím, kdy na úřad dorazí prostřednictvím e-podatelny písemnost, příslušný úředník ji však následně vytiskne a uloží do šanonu. Daný spis již po té po úřadě nebo i mezi úřady putuje v pouze v materiální podobě. To bohužel nebylo odstraněno ani Zákonem o archivnictví a spisové službě a o změně některých zákonů[12]. Na základě tohoto zákona je sice možné vést spisovou službu elektronicky, naneštěstí ale stále preferuje vedení spisové služby v podobě materiální před elektronickou.

[9] autora publikace „Úvod do eGovernmentu“
[10] Štědroň, B.: *Úvod do eGovernmentu*, Praha: Úřad vlády České republiky, 2007, str. 30
[11] Vnitřní procesy veřejné správy
[12] Zákon č. 499/2004 Sb.

Během prvního roku fungování ministerstvo financí dokonce pozastavilo práci na zajištění sdílení dat mezi jednotlivými registry a svou pozornost soustředilo na vytvoření portálu veřejné správy, portal.gov.cz – Na úřad přes internet. Portál veřejné správy se však stal pouze jakousi nástěnkou pro získávání informací z veřejné správy a o veřejné správě. Právě díky absenci možnosti sdílení dat ve veřejné správě se data určená pro tento portál musí speciálně vytvářet na zakázku. A to i přes to, že na portálu jsou zveřejňována data, která má již veřejná správa k dispozici.

O vyřešení tohoto problému se ministerstvo informatiky pokusilo prostřednictvím vypracováním věcného záměru návrhu zákona o sdílení dat při výkonu veřejné správy, který byl v roce 2004 předložen vládě. Přestože vláda tento věcný záměr svým usnesením[13] schválila a ministerstvo informatiky následně na jeho základě připravila i návrh zákona v paragrafovaném znění, bylo již pozdě a ministerstvo nestihlo legislativní změny prosadit do konce svého funkčního období. Pro navržené změny navíc nezískali ani podporu Legislativní rady vlády, takže se připravený materiál nedostal ani na samotné jednání vlády. Na následující vlády tak čeká práce na sdílení dat mezi jednotlivými registry zcela od začátku, vyjma možností využití některých dílčích dosavadních výsledků, jako např. analýzy a návrhu registru územní identifikace.

2.4 Možnosti zpřístupnění eGovernmentu občanům

Problémem zpřístupnění eGovernmentu může být pravděpodobně stále relativně vysoká cena připojení k internetu. V případě ADSL linky nelze mít tuto službu samostatně a je nutné mít k ní i jiné služby, což náklady na tento druh připojení zvyšuje. Od pořízení Wi-Fi zase mohou odrazovat vyšší pořizovací náklady spojené například s nákupem paraboly pro přijímání signálu. V současnosti je asi i proto trendem, že města a městské obvody zřizují místní nízko rychlostí Wi-Fi sítě s přístupem zdarma.

Dalším problémem se jeví počítačová negramotnost lidí. Z šetření, které uskutečnil Český statistický úřad ve 2. čtvrtletí 2006 vyplynulo, že i přes značný zájem o využívání služeb eGovernmentu (více než 60% občanů by tyto služby chtělo využívat) je více než polovina populace bez zkušeností s využíváním internetu a méně než 30% obyvatel má základní znalost práce s internetem.

Jedna z věcí, která naopak zpřístupnění k internetu, potažmo k eGovernmentu usnadňuje je neustále se snižující cena výpočetní techniky v poměru s reálným příjmem obyvatel.

[13] Usnesení č. 1064/2004

2.5 Komunikační kanály

Komunikační kanály informačních systémů veřejné správy (ISVS) můžeme podle typu komunikace rozdělit na tři typy:"[14] 1) G2G, 2) G2C a 3) občan-eGovernment (vše v rámci G2G a G2C realizované přes eGovernment).

Ideální by byla realizace tzv. „call centra", což by v praxi znamenalo existenci univerzální přepážky, která by občanům zajistila vyřešení běžných životních situací.

Mezi klasické komunikační kanály patří:

- **Osobní setkání –** osobní dostavení na konkrétní úřad je stále běžným způsobem komunikace s úřadem. Cílem eGovernmentu je nutnost navštívení úřadů co nejvíce eliminovat.
- **Informační kancelář –** slouží k poskytování informací jak při telefonických dotazech, tak při výše uvedených osobních setkáních.
- **Úřední deska –** každý úřad je podle zákona[15] povinen zřídit úřední desku, která musí být nepřetržitě veřejně přístupná. Obsah veřejné desky by měl být přístupný i způsobem umožňujícím dálkový přístup, čili na internetu. Na úředních deskách se publikují například vyhlášky a nařízení obcí apod.
- **Podatelna –** klasické podatelny fungují na každém úřadě a jejich účelem je příjem listin a dokumentů. Každý úředník je na požádání povinen potvrdit příjem příslušných listin
- **E-podatelna – „ve** *zjednodušené podobě se jedná o proces příjmu a archivaci elektronických zpráv."*[16] Všechny orgány veřejné správy mají zákonnou povinnost tyto podatelny provozovat.
- **Pošta (klasická)**
- **Média –** i média jako je televize, rádio nebo tisk poskytují veřejné správě široké spektrum komunikačních kanálů s občanem.
- **Internet –** do budoucna by se prostřednictvím e-mailu, webu nebo i IP telefonie měla odehrávat většina komunikace jak v rámci veřejné správy, tak mezi veřejnou správou a občany.

[14] O knize Úvod do eGovernmentu, http://www.ikaros.cz/node/4403, cit. [10. 4. 2008] online
[15] § 26 odst. 1 zákona 500/2004 Sb. správního řádu
[16] Elektronický podpis, elektronická podatelna a územní samosprávné celky. http://www.kr-vysocina.cz/vismo/dokumenty2.asp?u=450008&id_org=450008&id=918395&p1=0&p2=&p3=, cit. [15. 4. 2008] online

- **Vyvolávací systémy –** komunikační kanál, který slouží pro určení pořadí v případě, že se ve stejnou dobu obrací na orgány veřejné správy více žadatelů. Umožňuje i výstupy do internetu.
- **Interní oběžníky –** slouží k výměně informací mezi uzavřenou skupinou pracovníků
- **Intranet a Extranet –** počítačové sítě, které pracují na základě stejné technologie jako internet. Jsou to ale „soukromé“ sítě, takže možnost jejich využívání mají pouze malé skupiny uživatelů. Vnější přístup do takové sítě je zabezpečen a kontrolován. Jejich smyslem je sdílení informací a programů vybranými subjekty.
- **SMS brány a automatizované terminály –** do komunikačních kanálů patří i SMS brány nebo různé druhy informačních terminálů.

2.6 Specializované komunikační kanály v rámci ISVS

Některé specializované komunikační kanály v rámci ISVS:

- **ARES –** administrativní registr ekonomických subjektů.
  Na adrese http://wwwinfo.mfcr.cz/ares/ares.html umožňuje vyhledávání nad všemi ekonomickými subjekty registrovanými v ČR.
- **Databáze patentů a užitných vzorů –** na stránkách http://www.upv.cz je možné vyhledávání v databázi patentů, vynálezů a užitných vzorů přihlášených u Úřadu průmyslového vlastnictví.
- **Obchodní rejstřík -** http://www.justice.cz/, na těchto stránkách je možné vyhledávání v Obchodním rejstříku
- **Odcizená vozidla –** http://www.mvcr.cz/auta, prostřednictvím těchto stránek si může uživatel zkontrolovat, zda například automobil, který si chce koupit, není kradený.

2.7 Příklady přístupových zařízení

Telefony – nejjednodušší možností komunikace s úřadem je pravděpodobně to, že si na úřad zavoláte. Vyskytne se ale asi problém, že budete přepojování z jednoho úředníka na druhého. Vhodným řešením by bylo například call centrum, které by tuto komunikaci zjednodušilo. Tímto způsobem mohou být ale podávány pouze obecné informace, protože úředník má omezenou možnost zjistit s kým hovoří. Řešením by bylo ověření totožnosti například na základě dotazu na rodné číslo.

Osobní počítač – prakticky nejběžnějším způsobem přístupu k eGovernmentu je osobní počítač s připojením k internetu. U tohoto způsobu komunikace je možnost identifikace a autorizace zájemce například pomocí elektronického podpisu, díky tomu může být prostřednictvím tohoto kanálu uskutečněno i předání důvěrných informací.

Obdobou telefonického způsobu komunikace je používání aplikací jako je Skype a nebo ICQ, které například některé městské úřady v současnosti využívají.

Informační kiosky – před několika lety se začaly v České republice vyskytovat na veřejných místek, například nádražích nebo vstupních halách úřadů, informační kiosky. Kiosek je v podstatě standardní osobní počítač, ale v robustnějším provedení z důvodu větší odolnosti například proti vandalům. Kiosky jsou většinou vybaveny dotykovým displayem a autorizace u nich může probíhat například prostřednictvím chipové karty, jako je tomu v menze naší fakulty.

Mobilní přístupová zařízení – do oblasti využívání eGovernmentu v této oblasti spadají mobilní telefony a MDA, potažmo PDA. MDA a PDA jsou v podstatě kapesní počítače. Pomocí MDA, PDA a některých mobilních telefonů, je možné využívat služeb internetu. Dalším použitím jsou SMS o kterých se uvažuje jako o možnosti, jak varovat občany, například v případě povodní.

Veřejná přístupová místa – ne každý občan má doma možnost přístupu k internetu. Proto jsou například v některých městech místa (např. České Budějovice – náměstí Přemysla Otakara II.), kde má občan s notebookem nebo jiným zařízením podporujícím Wi-Fi možnost přístupu k internetu.

2.8 Zákon o eGovernmentu

Dne 25. 2. 2008 vláda schválila návrh zákona o eGovernmentu, 25. 3. 2008 byl návrh v 1. čtení projednán poslaneckou sněmovnou a na 1. 7. 2009 je plánováno nabytí účinnosti.

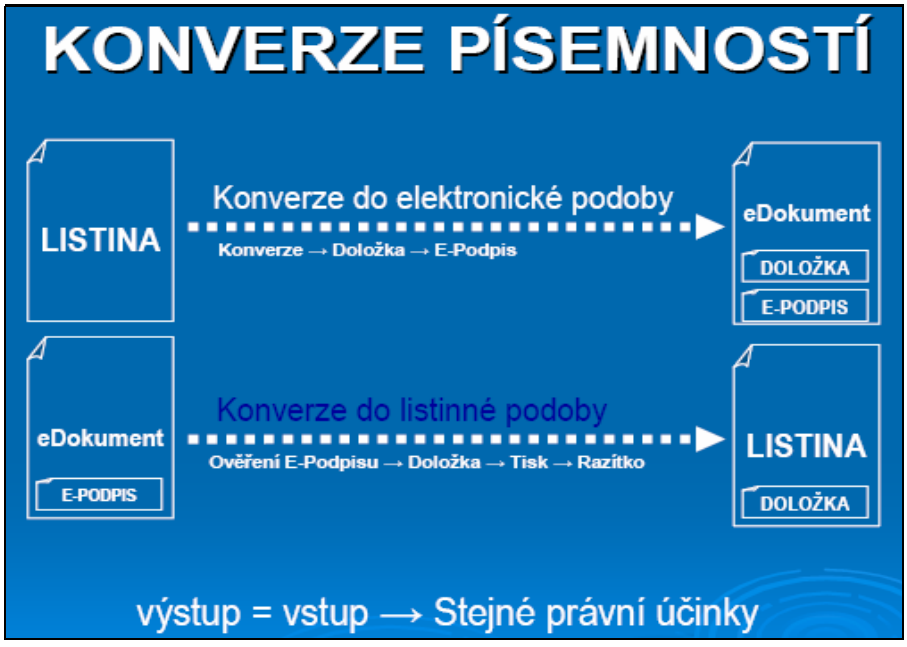
Tento zákon byl předložen ministerstvem vnitra spolu s ministerstvem spravedlnosti a zabývá se elektronickými úkony, osobními čísly a autorizovanou konverzí dokumentu. Podle vyjádření ministerstvem jde o přelomový a historický okamžik. Díky tomuto zákonu prý totiž bude možné úplně změnit a zefektivnit systém veřejné správy a to radikálním způsobem. Měl by nás přiblížit o krok blíže k modernímu a efektivnímu státu a bude tvořit srdce eGona, což je nový symbol moderní veřejné správy.

Zákon o eGovernmentu by měl přispět ke snížení byrokracie, k elektronizaci některých agend a k šetření času nejen úředníků ale i občanů. Papíry budou plnohodnotně nahrazeny spisy v elektronické podobě a ty by měli následně putovat jednotným systémem státní správy. Měla by tak opadnout nutnost vyplňování různých zbytečných formulářů. Ochrana osobních údajů by pak měla být zajišťována pomocí elektronického podpisu a systémem elektronické identity. Ochrana osobních údajů bude podle tvůrců zajišťována systémem elektronické identity a elektronickým podpisem.

Zákon počítá se zavedením povinné formy elektronické komunikace mezi orgány veřejné moci prostřednictvím datových schránek. Dále se počítá s povinnou formou elektronického doručování dokumentů orgánů veřejné správy fyzickým i právnickým osobám, které budou mít zpřístupněnou datovou schránku. Jedním z cílů zákona je konverze písemností do elektronické podoby. Jedná se v podstatě o převod písemností do systému DMS (document management system) či ECM (enterprise content management system).

Tímto zákonem by tedy měl být zvýšen výkon veřejné správy, minimalizována byrokracie pro občany a zavedena elektronická komunikace občanů s úřady a mezi úřady navzájem. Smyslem ale nemá být jen elektronizace jen některých agend, ale poskytnutí komplexního řešení pro všechny agendy vykonávané orgány veřejné moci.

Na obrázku 1 je názorně vidět proces konverze písemností, jeden z cílů zákona o eGovernmentu.



Obrázek 1: Konverze písemnosti
Zdroj: www.egovernment.cz

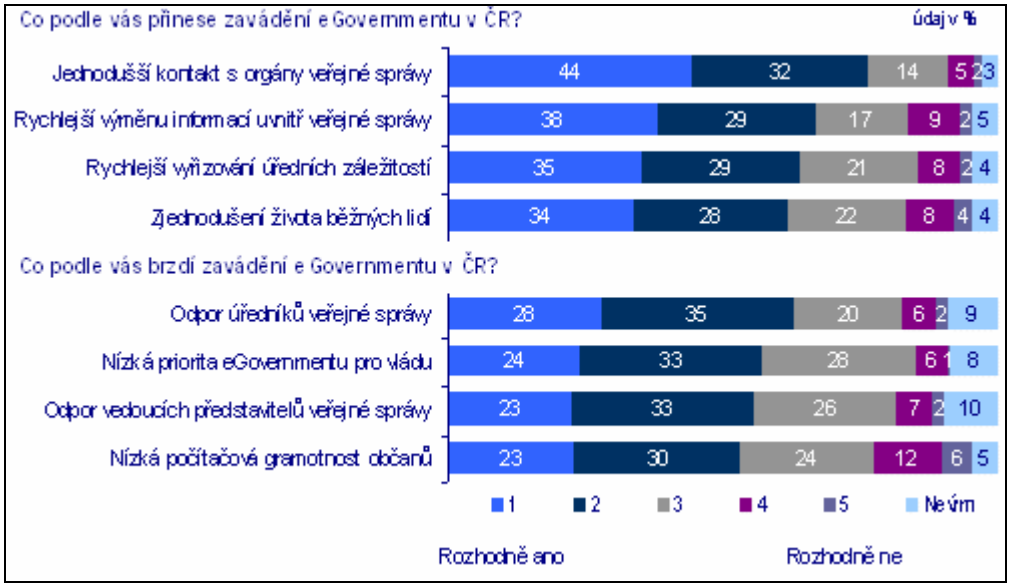
2.9 Aktuální postoje k eGovernmentu

Společnost Ipsos Tambor provedla začátkem roku 2008 výzkum na reprezentativním vzorku internetové populace ČR. Cílem bylo zjistit, jaké jsou aktuální postoje k eGovernmentu. Výzkum proběhl na základě spolupráce mezi společnostmi Ipsos Tambor a Microsoft Česká republika a to na vzorku 1020 uživatelů internetu, přičemž šlo hlavně o častější uživatele.

Všichni respondenti odpovídali na otázku, zda znají termín eGovernment. Jak je patrné z Grafu 1, 12 % z dotazovaných si tento termín spojuje s konkrétním obsahem. Dalších 14 % má o jeho obsahu alespoň přibližnou představu a celých 57 % o tomto termínu nikdy neslyšelo.

Následně se 12 % dotazovaných, kteří termín znali a dalších 14 %, kteří o tomto termínu měli alespoň představu, vyjadřovalo k očekáváním od eGovernmentu a hodnotili i možné brzdy jeho rozvoje. Z průzkumu vyplynulo, že respondenti od eGovernmentu očekávají především jednodušší kontakt s orgány veřejné správy a rychlejší výměnu informací uvnitř veřejné správy. Největší problém respondenti viděli v odporu samotných úředníků veřejné správy a nízké prioritě eGovernmentu pro vládu.

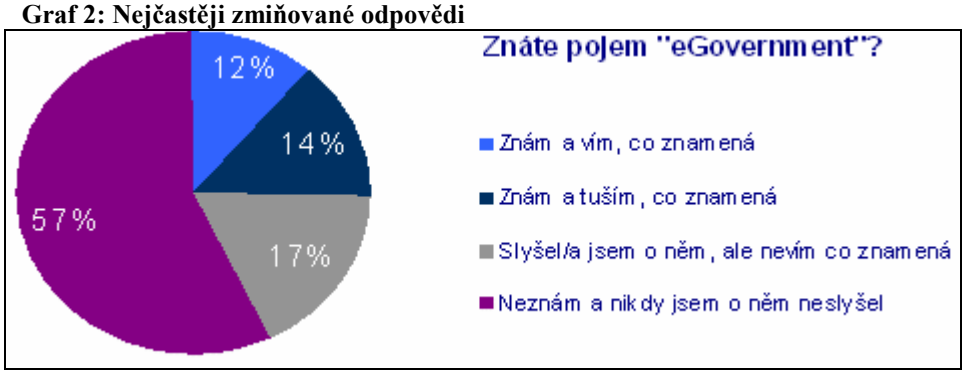
Graf 1: Znalost termínu eGovernment



Zdroj: www.marketingovenoviny.cz

Graf 2 shrnuje nejčastější odpovědi (respondenti měli vyjadřovat souhlas nebo nesouhlas s položkami zobrazenými vedle grafu)

Graf 2: Nejčastěji zmiňované odpovědi



Zdroj: www.marketingovenoviny.cz

2.10 Základní právní předpisy v rámci eGovernmentu

- zákon č. 71/1967 Sb., o správním řízení (správní řád), v platném znění (do 31. 12. 2005),
- zákon č. 500/2004 Sb., správní řád (s účinností od 1. 1. 2006),
- zákon č. 337/1992 Sb., o správě daní a poplatků, v platném znění,
- zákon č. 106/1999 Sb., o svobodném přístupu k informacím, v platném znění
- zákon č. 227/2000 Sb., o elektronickém podpisu, v platném znění,
- nařízení vlády č. 495/2004 Sb., k provedení zákona o elektronickém podpisu,
- vyhláška č. 496/2004 Sb., o elektronických podatelnách
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy, v platném znění,
- zákon č. 634/2004 Sb., o správních poplatcích,
- zákon č. 127/2005 Sb., o elektronických komunikacích
- zákon č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb

3 Projekty v oblasti elektronické komunikace

3.1 eGon

O eGovenmentu se mluví už dlouho, vládní představitelé tvrdí, že systém začne brzy fungovat, ale realita je bohužel odlišná. Zatím posledním projektem ministerstva vnitra je eGon, který nedávno oslavil své první narozeniny. Symbolem tohoto projektu je následující panáček eGon, který má mít stejně vlastnosti jako eGovernment samotný. Má být vstřícný, jednoduchý a funkční.

.

Obrázek 2: eGon

Tento panáček se stává novým průvodcem občana na cestě k veřejné správě a symbolem nového pojetí eGovernmentu.

eGon má čtyři části, prsty jeho rukou představují hustou kontaktní síť mezi úřady a občanem a tvoří je Czech POINTY. Oběhový systém představuje jednotnou komunikační infrastrukturu, srdce výkonné výpočetní systémy a zákon o eGovernmentu, a mozek je tvořen registry státní zprávy.

3.1.1 Czech POINT

3.1.1.1 Cíle projektu

Cílem tohoto projektu je vytvoření garantované služby pro komunikaci se státní správou prostřednictvím jednoho universálního místa, na kterém bude možné získat a ověřit data z veřejných i neveřejných informačních systémů, úředně ověřit dokumenty a listiny, převést písemné dokumenty do elektronické podoby a naopak, získat informace o průběhu správních řízení ve vztahu k občanovi a podat podání pro zahájení řízení správních orgánů. *„Jde tedy o maximální využití údajů ve vlastnictví státu tak, aby byly minimalizovány požadavky na občany.“*[17]

Projekt Czech POINT tak přináší významné ulehčení komunikace se státem. V některých situacích stačí dojít pouze na jeden úřad. Podle plánu tvůrců by v konečné fázi projektu občan mohl své záležitosti vyřizovat i z domova prostřednictvím internetu.

3.1.1.2 Kde Czech POINT najdeme

Czech POINTY můžeme v současnosti najít na 1390 obecních úřadech, 260 poštách, v 45 kancelářích Hospodářské komory a na 7 zastupitelských úřadech ČR v zahraničí. Do budoucna je plánován přístup i u notářů.

3.1.1.3 Co Czech POINT poskytuje

- **Výpis z Katastru nemovitostí** – o výpis může zažádat anonymní žadatel. Výpis lze žádat na základě listu vlastnictví nebo na základě seznamu nemovitostí. Žadatel musí znát buď katastrální území a číslo listu vlastnictví nebo katastrální území a parcelní číslo (případně číslo popisné). Vydání první strany výpisu je podle zákona zpoplatněno max. částkou 100, – Kč u dalších stran je tato maximální cena 50, – Kč.
- **Výpis z Obchodního rejstříku –** stejně jako u předcházejícího výpisu ho může požadovat anonymní žadatel. Výpis je možné požadovat na základě znalosti IČ obchodní organizace. Zpoplatnění je upraveno za stejných podmínek jako v předcházejícím případě.
- **Výpis z Živnostenského rejstříku –** vydávání a zpoplatnění je upraveno stejnými pravidly jako výpis z Obchodního rejstříku.

[17] Co je Czech POINT, http://www.czechpoint.cz/pages/oprojektu/cojeczechpoint.php.html, cit. [23. 4. 2008] online

- **Výpis z Rejstříku trestů –** výpis z Rejstříku trestů lze podle zákona vydat pouze osobě, které se tento výpis týká a to pouze na základě písemné žádosti. K vydání výpisu žadatel potřebuje platný doklad totožnosti a musí mu být přiděleno rodné číslo. Výpis lze vydat i na základě zplnomocnění. V případě, že je možné vyřídit tuto žádost o výpis z Rejstříku trestů elektronickou cestou, zaplatí žadatel podle zákona za tento výpis 50, – Kč jako správní poplatek. Výpis z rejstříku trestů je současnosti možné získat pouze na magistrátech, krajských a obecních úřadech.

3.1.1.4 Czech POINT E-SHOP – výpisy poštou

Česká pošta nedávno představila novinku, která ještě více přispěje k zjednodušení komunikace s veřejnou sférou. Nově je totiž možné objednat si výpisy z centrálních registrů elektronicky. Elektronicky lze požádat o výpis z Katastru nemovitostí, z Obchodního rejstříku a Živnostenského rejstříku.

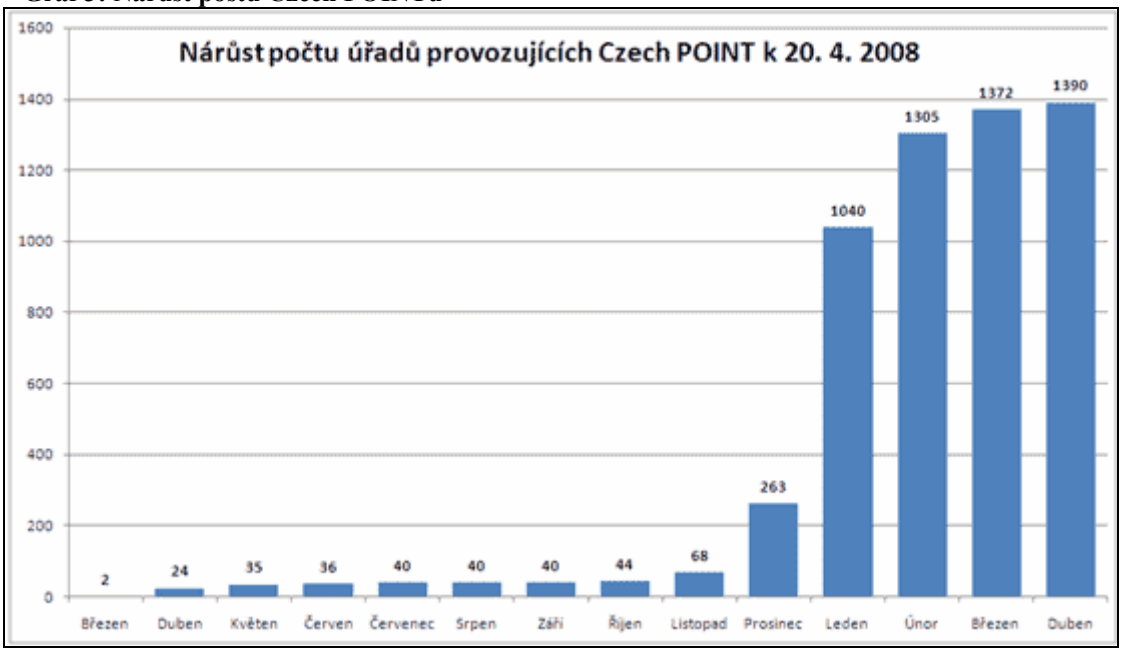
3.1.1.5 Čeho Czech POINTY dosáhli

Za dobu své činnosti se mohou pochlubit:

- 1390 starosty a jejich úřady, které se do tohoto projektu zapojily
- 6200 vyškolenými úředníky, kteří pomáhají občanům na kontaktních místech
- 7169 vydanými výstupy za jeden den, tento prozatímní rekord byl zaznamenán 26. 3. 2007
- 310 822 vydanými výstupy občanům za dobu fungování projektu (k 20. 4. 2008)

Jak je vidět v Grafu 3, k největšímu nárůstu počtu obecních úřadů zapojených do projektu Czech POINT došlo začátkem roku 2008.

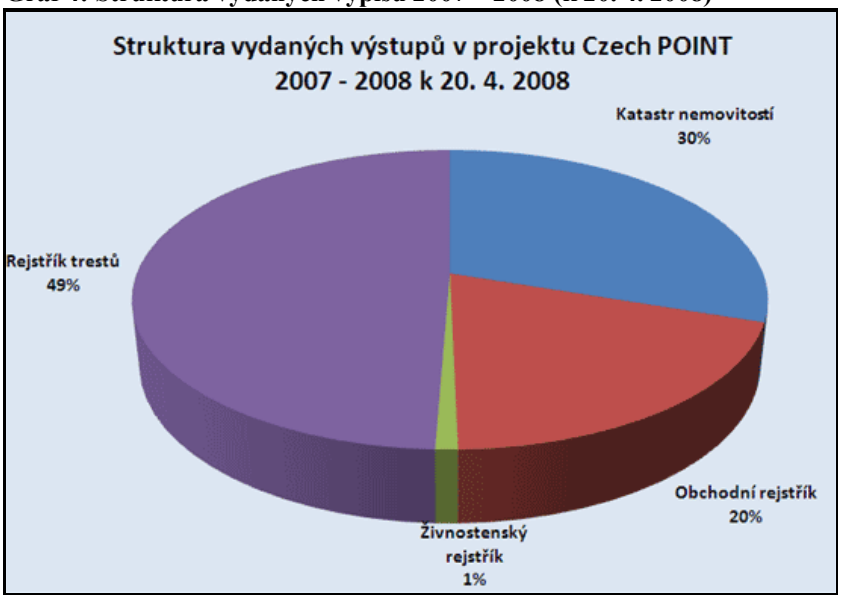
Graf 3: Nárůst poštu Czech POINTů



Zdroj: www.czechpoint.cz

V grafu 8 je znázorněna struktura vydaných výpisů za rok 2007 a část roku 2008. Z grafu vyplývá, že největší zájem je o výpisy z Rejstříku trestů, na druhém místě je výpis z Katastru nemovitostí následovaný Obchodním rejstříkem. Živnostenský rejstřík je s 1 % pro uživatele služby nejméně zajímavý.

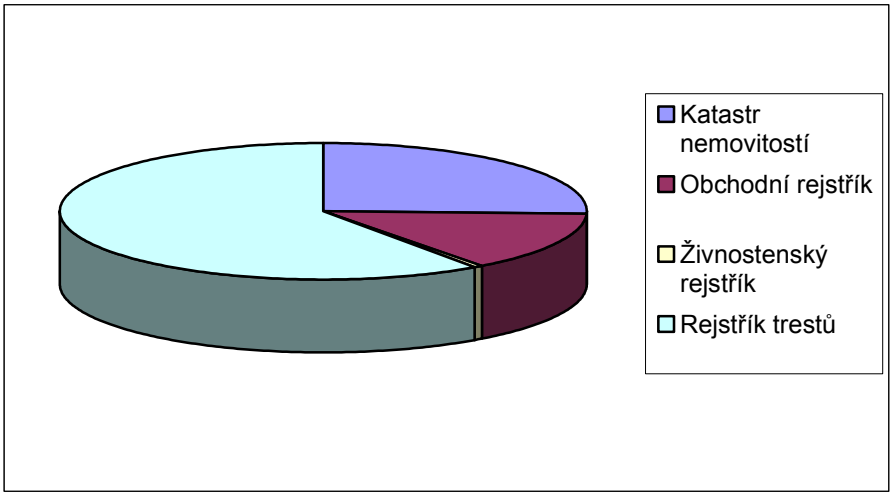
Graf 4: Struktura vydaných výpisů 2007 – 2008 (k 20. 4. 2008)



Zdroj: www.czechpoint.cz

Předchozí graf je ale nepřesný, výpisy z Rejstříku trestů jsou totiž vydávány až od začátku roku 2008. Graf 4 zobrazuje, jak vypadá struktura vydaných výpisů k 20. 4. 2008. Je z něj jasné patrné, že bezkonkurenčně největší zájem byl v první třetině roku o výpisy z Rejstříku trestů.

Graf 5:Struktura vydaných výpisů 2008 (k 20. 4. 2008)



Zdroj: vlastní tvorba

3.1.1.6 Plány na rok 2008

Na letošní rok se v oblasti toho projektu plánuje novela živnostenského zákona. Novela by se měla týkat zprostředkování žádosti o živnost a podacího terminálu. Dalšími plány jsou jednotný identitní prostor, který počítá s integrací s ePUSA[18] a samosprávnými agendami, a výpisy z registru bodů řidiče a hlášení matričních událostí do evidence obyvatel. Posledním plánem je příprava na platnost eGa, což bude ověřovací terminál konverze dokumentů.

3.1.2 Registry státní zprávy

Zastřešující zákon o základních registrech byl rozeslán do mezirezortního připomínkového řízení. Předpoklad nabytí účinnosti je stanoven na 1. 7. 2009. V přípravě jsou i novely zákonů, které upraví konkrétní základní registry. U těchto novel je předpokládaná účinnost od 1. 1. 2010.

Základními registry budou registr osob; registr územní identifikace, adres a nemovitostí; registr práv a povinností; registr obyvatel.

[18] elektronický portál územních samospráv provozovaný Ministerstvem vnitra.

3.2 VIRTUOS

3.2.1 Vysvětlení pojmu

Virtuos[19] je projekt Plzeňského kraje za 40 mil. Kč, který byl zahájen 2. 4. 2008 a je z 75 % financován z fondů EU. Jeho cílem je vytvořit informační systém portálového typu, který by umožnil elektronickou komunikaci občanů s veřejnou správou a současně také elektronickou komunikaci mezi úřady navzájem. Dalším cílem je dát tento informační systém k dispozici všem městům a obcím v kraji a následně i v celé ČR.

K tomuto projektu kraj inspiroval fakt, že pokud občané něco řeší s veřejnou správou, je to nejčastěji prostřednictvím městského nebo obecního úřadu.

„Centrální státní správa řeší elektronizaci především těch agend, které sama přímo vykonává, výjimečně i těch, které pro ni vykonávají v přenesené působnosti města a obce.“[20] Města a obce ale nemají dostatek finančních prostředků na to, aby si individuálně řešily svou elektronickou komunikaci s občany. Vedení Plzeňského kraje tedy před více než dvěma lety došlo, že je nesmysl čekat a spoléhat se na to, že se stát kromě své vlastní el. komunikace s občany začne zajímat i o el. komunikaci s úřady měst a obcí. A tak se zrodil projekt Virtuos.

3.2.2 Co nabízí

Z přibližně 800 typů nejrůznějších podání jich bude VIRTUOS řešit 70. Postupně by se měl tento počet s vývojem související legislativy navyšovat. Těmito možnými podáními by například mělo přihlášení psa do obecního registru, ohlášení drobné stavby nebo stavební úpravy či oznámení matrice změny např. v případě sňatku. Systém bude rovněž připraven i na platby správních poplatku prostřednictvím SMS.

3.2.3 Co je třeba k využívání

Zájemci o využívání tohoto systému nejdříve musí na internetové stránce projektu www.eVirtuos.cz vyplnit žádost o registraci a následně na příslušném úřadu podepsat smlouvu. Poté už lze s úřadem z velké části komunikovat elektronicky. Majitelé elektronického podpisu, nemusí na úřad ani kvůli sepsání smlouvy.

[19] www.evirtuos.cz
[20] Virtuos přináší výhody i malým sídlům, http://moderniobec.ihned.cz/c4-10024680-23728720-C00000_d-virtuos-prinasi-vyhody-i-malym-sidlum, cit. [4. 4. 2008] online

3.2.4 Výhody pro občany

Občanům především umožní přestat chodit na úřad a tam kde je to možné, vyřídit příslušnou záležitost elektronicky. Systém však umožňuje i rezervaci času na přepážce nebo dokonce přímo u konkrétního úředníka. To vše v případě, že občan na úřad opravdu musí.

Další možností systému, je sledování co se s konkrétním podáním v rámci správního řízení děje. Tato možnost se vztahuje jak na elektronická podání, tak i na klasicky vyřizované záležitost. Z pohledu občana se tento projekt asi nejvíce podobá internetovému bankovnictví.

K dnešnímu dni (tj. 21. dubna) je v projektu registrováno 84 uživatelů.

3.2.5 Výhody pro obce

Úřadům, které nemají žádný vnitřní agendový informační systém, ani žádný portál k elektronické komunikaci s občany, umožňuje komplexní řešení jejich potřeb. Samozřejmostí jsou i funkce potřebné ke splnění zákonných povinností měst a obcí, jako je elektronická podatelna, elektronická úřední deska nebo jednoduchý informační portál pro obce bez vlastních internetových stránek.

K dnešnímu dni (tj. 21. dubna) je v projektu registrováno 5 obcí.

3.2.6 Budoucnost

Pozice informačního systému Virtuos ve veřejné správě do budoucna je asi nejlépe charakterizována dvěma skutečnostmi. *„První je jeho vnímání ministerstvem vnitra, které v něm vidí vhodný nástroj pro praktické zabezpečení elektronické komunikace mezi občany a samosprávou.“*[21] Tuto skutečnost vystihuje i ministerský slogan „Kde je samospráva, je i Virtuos, a kde je Virtuos, tam je Czech Point – a naopak“

Virtuos má tedy ambice stát se informačním systémem, který bude řešit elektronickou komunikaci v samostatné a z větší části i přenesené působnosti vykonávané městy a obcemi. Jeho poloha je přitom přesně v rámci principu systému Czech POINT.

Druhou podstatnou skutečností z hlediska jeho budoucnosti je fakt, že figuruje na seznamu zhruba osmi společných projektů, na nichž se shodly příslušné subkomise a komise Asociace krajů ČR a Svazu měst a obcí ČR.

VIRTUOS se tedy chce stát informačním systémem, který řeší elektronickou komunikaci v samostatné a z větší části i přenesené působnosti vykonávané městy a obcemi. Jeho poloha

[21] Virtuos přináší výhody i malým sídlům, http://moderniobec.ihned.cz/c4-10024680-23728720-C00000_d-virtuos-prinasi-vyhody-i-malym-sidlum, cit. [4. 4. 2008] online

je přesně v rámci principů aplikovaných systémem Czech POINT, a to včetně jeho budoucího rozvoje.

3.3 Portál veřejné správy

3.3.1 Vysvětlení pojmu

„Portál veřejné správy[22] (dále PVS) *slouží jako zdroj informací a rozcestník, který vede na stránky ministerstev a státních úřadů.“*[23] Je spravován ministerstvem vnitra a jeho hlavním smyslem je pomoci občanům a firmám při orientaci a komunikaci s úřady veřejné správy. Jinými slovy řečeno, jde tedy o informační systém, který je provozován za účelem usnadnění vzdáleného přístupu k informacím z veřejné správy.

Portál má dvě funkce:

- **Transakční** – slouží k výměně dat nebo informací. Je určena jak institucím, tak občanům a umožňuje jednotný přístup k elektronickým službám.
- **Informativní** – tato část je určena výhradně občanům, právnickým osobám nebo cizincům, kteří mají co dočinění s českými úřady.

3.3.2 Informační část

V této části portálu je možno nalézt novinky z veřejné správy, z portálu samotného nebo obecné informace o České republice. Pokud má uživatel zájem o konkrétnější informace, může si vybrat z rubrik adresář, zákony, mapy a životní situace.

- **Adresář** – je v podstatě seznam orgánů veřejné správy a správních měst a obcí. Je zde možné najít spoustu důležitých informací a zajímavostí. Zdrojem těchto informací je Český statistický úřad.
- **Zákony** – cílem této části portálu zpřístupnění platné legislativy České republiky a EU. Zákony v této sekci jsou volně ke stažení.
- **Mapy** – tvoří vstupní bránu k územně vázaným informacím.
- **Životní situace** - *„Tato sekce, slouží k usnadnění každodenního života občanů, cizinců a podnikatelů. Je to obdoba sekcí „Co mám dělat když...?“, které jsou běžné na stránkách měst a obcí.“*[24] K nalezení jsou zde například metodické návody pro komunikaci s úřady.

[22] www.portal.gov.cz
[23] Počítač pro každého: *Kudy na úřad přes internet*, č. 9/2006, str. 42
[24] Portál veřejné správy – k čemu je nebo může být, http://www.isvs.cz/portal-gov-cz/portal-verejne-spravy-k-cemu-je-nebo-muze-byt-1-dil.html, cit. [6. 4. 2008] online

3.3.2.1 Uživatelské role

Uživatelské role povyšují PVS na něco jiného než pouze na seznam kontaktů na úřady. Každý návštěvník má možnost zvolit mezi uživatelskou rolí občana, podnikatele nebo cizince.

Tabulka 1: Témata k výběru podle jednotlivých rolí

Občan	Podnikatel	Cizinec
Rodina	Podnikatelská činnost	Než přijedete do ČR
Občan-Obec-Stát-EU	Dotace, podpůrné programy	Pobyt na území ČR
Bydlení	Veřejné zakázky	Zaměstnání
Zaměstnání	Právo a finance	Podnikání
Doprava a cestování	Rozvoj podnikání	Systém školství a uznávání vzdělání
Vzdělávání, věda, kultura	Daňový systém	Systém zdravotnictví a zdravotního pojištění
Zdraví	Pracovně právní vztahy	Systém soc. zabezpečení
Životní prostředí	Informace o tržním prostředí	Rodina, manželství a životní události

3.3.3 Transakční část

Tato část portálu slouží především k elektronické komunikaci mezi občany (firmami) a orgány veřejné správy, případně ke komunikaci mezi orgány navzájem. Jejím primárním cílem je umožnit vyřízení co nejširšího okruhu agend elektronicky, tzn., aby občan nebo firma nemuseli podávat „papírové“ formuláře či výkazy, ale mohli tyto informace předávat příslušným orgánům elektronickou cestou.

K elektronickému podávání je třeba registrace uživatele. Pokud se uživatel úspěšně zaregistruje, získá možnost elektronicky odesílat a přijímat formuláře z úřadů veřejné správy a to s využitím identifikátoru uživatele nebo digitálního certifikátu.

3.3.3.1 Podání

Podání je důležitou součástí portálu. Slouží k elektronické komunikaci mezi občany resp. organizacemi a orgány veřejné správy. Většinu kapacity transakční části portálu však využívají úřady pro vzájemnou komunikaci mezi sebou.

3.3.3.2 Nabízené elektronické služby

PVS v současnosti nabízí tyto služby:

- **Služby České správy sociálního zabezpečení**
  - Evidenční listy důchodového pojištění
  - Přihlášky (odhlášky) zaměstnanců k nemocenskému pojištění
  - Přehled o příjmech a výdajích OSVČ

- **Služby ministerstva průmyslu a obchodu**
  - Roční výkaz o poštovních službách PS
- **Služby ministerstva financí**
  - Daňové přiznání z příjmu fyzických osob typ A a B
  - Daňové přiznání z příjmu právnických osob
  - Přiznání k dani z přidané hodnoty
  - Daňové přiznání k dani silniční
  - Daňové přiznání k dani z nemovitostí
  - Oznámení o nezdaněných vyplacených částkách fyzickým osobám
  - Obecná písemnost
- **Služby Generálního ředitelství cel**
  - Daňová přiznání ke spotřebním daním
- **Ministerstvo dopravy – „***Ministerstvo dopravy využívá PVS při vyhodnocování testů uchazečů o řidičské oprávnění. Komisaři odesílají výsledky do centrály, kde jsou počítačem vyhodnoceny.“*[25]
- **Ministerstvo životního prostředí**
  - Ohlášení znečištění

3.3.3.3 Registrace

Pro využívání jakékoli služby e-podání na PVS je třeba registrace. Registraci lze provést buď jako občan, organizace a nebo zástupce. Od zvoleného typu uživatelské role se odvíjí i způsob identifikace, který bude od PVS vyžadován. K identifikaci lze použít buď uživatelský identifikátor, který představuje nižší zabezpečení, nebo certifikát.

Uživatelský identifikátor – umožňuje společně s heslem přistupovat uživatelům k již zaregistrovaným službám. Uživatel ho obdrží po zadání a ověření požadovaných informací při první registraci v aplikaci Elektronická podání, nebo když se chce poprvé přihlásit k odběru nějaké vybrané služby. Po úspěšném přihlášení se tento identifikátor používá k přístupu k dalším.

Certifikát – datová struktura, která je vydána důvěryhodnou institucí na omezenou dobu, a která zajišťuje mechanismus provázání veřejných a soukromých klíčů. Používá se jako

[25] Portál veřejné správy – elektronická podání, http://www.isvs.cz/portal-gov-cz/portal-verejne-spravy-elektronicka-podani-7-dil.html, cit. [7. 4. 2008] online

záruka identity, ale také k ochraně informací posílaných přes Internet. Certifikát je některými službami poskytovanými PVS vyžadován.

3.3.3.4 Zabezpečení

Na PVS je k zabezpečení přenášených dat kromě již zmiňovaných uživatelských identifikátorů a certifikátů použito i zabezpečení připojení. To v praxi znamená, že všechny informace, které jsou přijaty nebo poslány, jsou přenášeny přes 128bitové zabezpečení připojení (SSL). Na stránkách PVS je zmíněno, že dalším bezpečnostním prvkem je šifrování. O které šifrování se jedná, ale zmíněno není a musíme se tedy spokojit s oznámením, že šifrování je „v souladu s nejvyššími standardy“.

3.4 Soutěže v oblasti eGovermentu

3.4.1 Úvod

Existuje řada soutěží, ve kterých jsou posuzovány nejlepší projekty v oblasti veřejné správy, respektive eGovermentu. Jako příklad takové soutěže lze uvést Zlatý erb, soutěž, ve které se každoročně hodnotí nejlepší webové stránky a elektronické služby měst, obcí a krajů. Letos byl v rámci konference ISSS[26] vyhlášen již jubilejní 10. ročník.

Dalším příkladem je Egovernment The Best, kterým jsem se rozhodl zabývat podrobněji.

3.4.2 Egovernment The Best

Stejně jako v roce 2006 redakce magazínu Egovernment zveřejnila na sklonku minulého roku nejzajímavější projekty elektronizace veřejné správy. Ze všech čtenářských námětů byla vybrána dvacítka nejzajímavějších projektů či realizací, jejichž charakter odpovídal myšlence elektronizace veřejné správy, byly aktuální a navíc splňovaly kritéria výběru.

3.4.3 Kritéria výběru

Ohledně kritérií se redakce inspirovala soutěží European eGovernment Awards.

Jedná se především o:

- **prokazatelnost účinků a vlivu projektu (30 bodů) –** např. **„***kvantitativní a kvalitativní doložení dopadu nebo výsledků“*[27]
- **prokazatelnost potenciálu pro využití projektu (20 bodů)** – jak až je dané řešení přenositelné a realizovatelné pro ostatní.
- **pochopení „vícekanálových“ aspektů (20 bodů) –** *„jak je v projektu využit „vícekanálový“ přístup, respektive v jakém poměru je on-line a off-line dodávka služeb a osobní dodávka služeb.“*[28]
- **zlepšení a účinnost řízení (20 bodů) –** zda je použití přístup v nějakém ohledu inovační
- **celkový dojem a komunikační schopnost (10 bodů)** – zda je řešení projektu něčím výjimečné a zda je způsob prezentace působivý

3.4.4 Kdo výběr provádí

Prvotní výběr zajímavých projektů provádí redakce magazínu Egovernment. Tento výběr se uskutečňuje především na základě prezentací na různých konferencí a na základě tipů od

[26] Internet ve státní správě a samosprávě, www.isss.cz
[27] Kritéria hodnocení, http://www.egovernment.cz/best/kriteria.htm, cit. [7. 4. 2008] online
[28] Egovernment The Best 2007, http://egovernment.cz/best/PDF%2007/cela%2007.pdf, cit. [7. 4. 2008]

čtenářů. Vybrané projekty jsou dále konzultovány s odborníky z ministerstva vnitra, Svazu měst a obcí ČR, SPIS a v neposlední řadě s odborným partnerem, se společností KPMG.

3.4.5 Vyhodnocení The Best 2007

Ze zmiňovaných dvaceti projektů byly nakonec vybrány tři nejlepší. Na prvním místě se umístil již zmiňovaný projekt „Czech POINT“ ministerstva vnitra. Druhé místo obsadil „InfoSoud“ ministerstva spravedlnosti a jako třetí nejlepší řešení byla vyhodnocena „Příprava materiálů v elektronické podobě pro jednání rady města a zastupitelstva města“ města Uherský Brod.

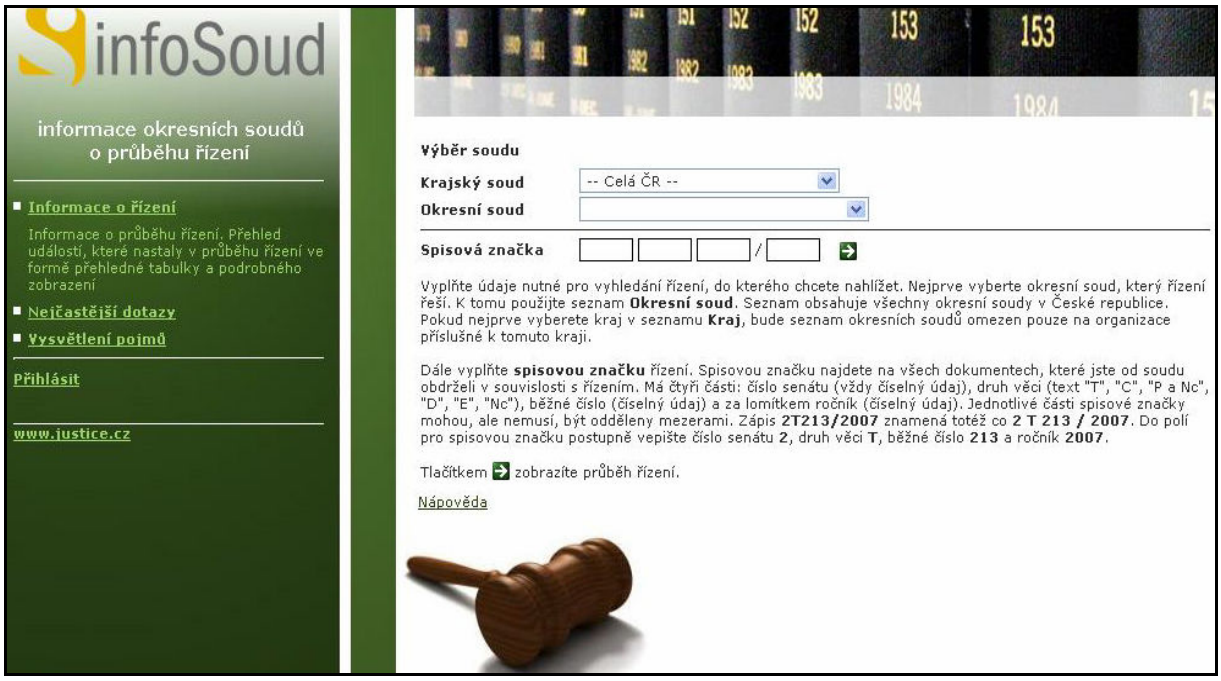
3.4.5.1 Czech POINT

Projekt byl již popsán výše, zaměřím se tedy pouze na dva další projekty.

3.4.5.2 InfoSoud

3.4.5.2.1 Úvod

InfoSoud je projekt ministerstva spravedlnosti, jehož ostrý provoz byl spuštěn 7. dubna 2008. Ministerstvo mělo při zkušebním rozběhnutí projektu problém s doménou infosoud.cz, která se dostala do rukou soukromé společnosti EPravo.cz dříve, než si ji stihlo ministerstvo spravedlnosti zaregistrovat. Služba infoSoud v současnosti funguje na adrese www.infosoud.justice.cz. Podle posledních informací, by ale i doména infosoud.cz měla přejít do vlastnictví ministerstva a bude fungovat na bázi přesměrování na současnou adresu.



Obrázek 3: Ukázka webu infosoudu
Zdroj: www.infosoud.justice.cz

3.4.5.2.2 Co nabízí

Účastníci řízení se prostřednictvím této internetové služby mohou dostat k informacím ohledně průběhu jejich vlastních sporů. Šetří se tak jejich čas a navíc to přispívá ke snížení zatížeností kanceláří soudů, protože ubývá např. telefonických dotazů o postupu řízení.

Přehledné informace o stavu projednání případu získají zájemci na základě zadání příslušného jednacího čísla. Zveřejňovány jsou ale pouze takové informace, které účastníkům umožňují sledování postupu ve vyřizování věci. Osobní údaje k dispozici nejsou.

3.4.5.2.3 Princip fungování

Jednotlivé krajské a okresní soudy zasílají každý den informace o svých evidovaných řízeních na server s úložištěm dat, který následně zprostředkovává přístup k těmto údajům veřejnosti. Pro tyto účely byl implementován komunikační modul do systému dílčích organizací, který se aktivuje jednou denně. Jeho úkolem je projít nově zapsané informace, vybrat ty ke zveřejnění a předat je do centrálního úložiště. Následně překontroluje úspěšnost procesu, v případě nutnosti zašle data opakovaně.

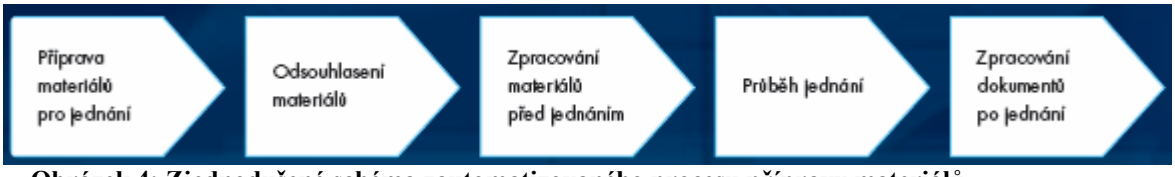
Jádro celého systému tvoří centrální evidence stavů věcí, prostřednictvím které je realizováno shromažďování dat organizací a jejich poskytování k prezentaci přes webové rozhraní. U každého spisu je evidována spisová značka, organizace, jíž spis náleží, seznam stavů věci a seznam jednání ve věci. Pro každý spis se dále chronologicky zaznamenává průběh stavů věci.

3.4.5.3 Příprava materiálů v elektronické podobě

3.4.5.3.1 Úvod

Rozsahem menší ale přesto neméně zajímavý projekt je „Příprava materiálů v elektronické podobě pro jednání rady města a zastupitelstva města“.

Přínosem tohoto projektu je zefektivnění fungování rady a zastupitelstva Uherského Brodu a to prostřednictvím zautomatizování procesu, který zobrazen na následujícím obrázku.



Obrázek 4: Zjednodušené schéma zautomatizovaného procesu přípravy materiálů
Zdroj: www.egovernment.cz

Jako softwarový nástroj pro přípravu dokumentů město zvolilo aplikaci Dokumenty zastupitelstva a rady (DZR), kterou dodala společnost ADVICE.CZ. Tento software *„sjednotil, zrychlil a usnadnil městu proces vzniku nových dokumentů a nakládání s těmi stávajícími.“*[29]

3.4.5.3.2 Základní schéma procesů

Přípravu materiálů pro jednání tvoří elektronizace podoby materiálu prostřednictvím výše zmiňované aplikace, vyplnění titulního listu každého bodu jednání, ve kterém je specifikováno např. s kým byl daný materiál projednán nebo je vkládána tématická oblast pro pozdější snadnější orientaci v uložených materiálech. Po těchto úkonech následuje strukturovaná formulace návrhu usnesení, kde jsou definováni předkladatelé, případně spoluzpracovatelé materiálu. Definice předkladatele je důležitá při odesílání materiálu k odsouhlasení a při jeho předávání do programu jednání.

I odsouhlasení materiálu probíhá elektronickou formou. Předkladateli jsou doručeny informace o vloženém materiálu e-mailem, který obsahuje mimo jiné i aktivní odkaz, jehož prostřednictvím se předkladatel může dostat přímo k zaslanému materiálu. Po odsouhlasení materiálu předkladatelem je o této skutečnosti stejnou formou informován správce systému, který příslušný materiál přebírá k dalšímu zpracování.

Správce systému provádí zpracování materiálů, které se skládá z formální kontroly materiálů, sestavení programu jednaní, kompletace návrhů usnesení a distribuce materiálů členům Rady města.

Fáze zpracování dokumentů po jednání představuje vytvoření finální podoby zápisu z jednání, formulace a ověření jednotlivých usnesení, a následného zveřejnění plné verze na intranetu a verze, která je v plném souladu se zákonem o ochraně osobních údajů na internetu.

3.4.5.3.3 Distribuce materiálů

Materiály připravené v systému DZR se dělí na řádné a na materiály tzv. na stůl.

Řádné materiály jsou distribuovány členům Rady města prostřednictvím CD, která jsou zašifrována a jsou čitelná pouze na noteboocích členů Rady města. Každý z členů je vybaven osobním tokenem s osobním šifrovacím certifikátem, jehož prostřednictvím předaný materiál rozšifruje.

[29] Byly vyhlášeny výsledky soutěže egovernment the best, http://www.isvs.cz/e-government/byly-vyhlaseny-vysledky-souteze-e-government-the-best-2007.html, cit. [8. 4. 2008] online

„Distribuce materiálů „na stůl“ je řešena prostřednictvím jednorázové synchronizace potřebných souborů“ [30]ze serveru městského úřadu s notebooky členů Rady města, která je realizována prostřednictvím Wi-Fi sítě, nainstalované v zasedací místnosti. Ve výjimečných případech je potřeba rozdělovat i materiály, které vzniknou v průběhu jednání Rady města. I jejich distribuce je zajištěna interní Wi-Fi sítí.

Proces přípravy materiálů na jednání Rady města i Zastupitelstva města probíhá shodně. Rozdíl spočívá pouze v distribuci. Materiály pro Zastupitelstvo města jsou stále distribuovány v papírově podobě, protože ne všichni členové zastupitelstva jsou zatím vybaveni potřebnou technikou.

[30] Egovernment The Best 2007, http://egovernment.cz/best/PDF%2007/cela%2007.pdf, cit. [8. 4. 2008]

4 Bezpečnost v elektronické komunikaci

4.1 Ochrana PC

Komunikace prostřednictvím e-mailu a dalších aplikací není v žádném případě ideálem bezpečnosti. Tyto aplikace jsou středem pozornosti pro viry, trojské koně a tzv. červy.

Viry jsou malé kousky kódů, které se nahrávají do paměti spuštěného počítače a následně připojují svůj kód ke všem programům, které jsou následně spuštěny. Viry se obvykle soustřeďují na spustitelné soubory a jejich činnost se projevuje například zpomalenou funkcí počítače nebo ztrácením dat.

Trojské koně jsou programy, které uživatel spustí v dobré víře a které následně odesílají osobní data a hesla svému tvůrci. Mohou mít podobu například totožně vypadajícího okna pro přihlášení uživatele, s tím rozdílem, že vyplnění a následné potvrzení nevede k přihlášení, ale k odeslání dat tvůrci trojského koně.

„*Červy jsou programy, které se samy znovu a znovu replikují, ale ve skutečnosti programy nenakazí.*“[31] Jejich obvyklým způsobem šíření je jejich automatické rozesílání na všechny kontakty v adresáři e-mailové schránky.

Obrana je proti těmto druhům virů je v podstatě velmi jednoduchá. Kontrolovat všechny přílohy v e-mailech pomocí antivirových programů a hlavně žádné podezřelé přílohy neotvírat. Jde zejména o spustitelné přílohy, tzn. s příponou .exe, .bat, .com apod. Nebezpečné mohou být ale i přílohy s příponou .doc, .xls, které mohou obsahovat tzv. makroviry.

Zmiňované antivirové programy mají rezidentní monitorovací část, která se spustí spolu s počítačem, nahraje se do paměti a následně zkoumá všechny spuštěné programy na přítomnost virů. V případě nalezení nakaženého souboru, je jeho spuštění zastaveno a dána nabídka na jeho smazání a nebo pokus o jeho vyléčení. Další funkcí antivirových programů je možnost prověření lokálních disků nebo jiných médií na přítomnost virové infekce.

Firewall, pod tímto pojmem se skrývá systém, který kontroluje komunikaci mezi internetovým prostředím a počítačem, případně počítačovou sítí. Skládá se ze dvou základních částí. Části, která blokuje data a druhé, která je povoluje. Jeho cílem je umožnit uživatelům lokálních sítí přístup do internetu, ale zároveň zabránit opačnému přístupu, tedy z internetu do lokální sítě. Tím firewall chrání počítač například proti útokům hackerů.

[31] Rybka, M., Malý, O.: *Jak komunikovat elektronicky*, Grada, 2002, str. 51

4.2 Zabezpečení komunikace v rámci eGovernmentu

4.2.1 Související pojmy

- **Podepisující osoba** – *„fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby.“*[32]
- **Elektronický podpis** – jeden hlavních nástrojů identifikace a autentizace osob na internetu. Podle zákona o elektronickém podpisu jím může být i „běžný podpis“ v textu emailu.
- **Zaručený elektronický podpis** – *„Zaručený elektronický podpis jsou tedy digitální data, která podepisující vytvoří pomocí svého soukromého klíče a zajišťuje jimi integritu a nepopiratelnost podpisu podepsaných dat.“*[33]
- **Uznávaný (zaručený) elektronický podpis** – zaručený elektronický podpis, který je založen na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb. Pouze tento typ certifikátů lze na základě zákona o elektronickém podpisu použít při komunikaci s orgány veřejné moci.
- **Kvalifikovaný certifikát** – certifikát, který byl vydán kvalifikovaným poskytovatelem certifikačních služeb a splňuje náležitosti stanovené zákonem o elektronickém podpisu. Slouží ke zveřejnění dat pro ověření elektronického podpisu a k jejich spojení s osobou, která podepisuje (tzv. veřejný klíč).
- **Kvalifikovaný systémový certifikát** – zjednodušeně řečeno, kvalifikovaný certifikát určený pro organizace.
- **Elektronická značka (el. razítko)** – jedná se o obdobu elektronického podpisu, která se liší zejména po právní stránce. Při tvorbě elektronické značky není nutné, aby bylo každé její vytvoření osobně odsouhlaseno, ale může být vytvářena i automatizovaně. To odstraňuje vázanost podpisu na konkrétní osobu. Vytváří se prostřednictvím kvalifikovaného systémového certifikátu.
- **Kvalifikované časové razítko** – datová zpráva vydaná kvalifikovaným poskytovatelem certifikačních služeb. Umožňuje důvěryhodné spojení dat v elektronické podobě s časovým okamžikem. Tím zaručuje, že uvedená elektronická data existovala již před daným časovým okamžikem.

---

[32] Štědroň, B.: *Úvod do eGovernmentu*, Praha: Úřad vlády České republiky, 2007, str. 15

[33] Elektronický podpis, elektronická podatelna a územní samosprávné celky. http://www.kr-vysocina.cz/vismo/dokumenty2.asp?u=450008&id_org=450008&id=918395&p1=0&p2=&p3=, cit. [15. 4. 2008] online

- **Poskytovatel certifikačních služeb (certifikační autorita)** – fyzická nebo právnická osoba, případně organizační složka státu, která vydává certifikáty nebo jiné služby spojené s e-podpisy a vede jejich evidenci.
- **Akreditovaný poskytovatel certifikačních služeb (akreditovaná cert. autorita)** – poskytovatel, který splňuje podmínky uvedené v zákoně o elektronickém podpisu pro výkon akreditovaného poskytovatele certifikačních služeb.
- **CRL (Certification Revocation List)** – seznam zneplatněných certifikátů vydávaný v pravidelných intervalech certifikační autoritou. V tomto seznamu jsou zapsány informace o těch certifikátech, které jejich majitelé nechali zneplatnit.

4.2.2 Úvod

Zákon o elektronickém podpisu, schválený v roce 2000, upravuje používání elektronického podpisu, elektronické značky, poskytování certifikačních služeb a dalších souvisejících služeb poskytovateli se sídlem na území České republiky. Nutnou podmínkou pro komunikaci občanů s orgány státní správy elektronickou cestou je dle zákona využití tzv. kvalifikovaného elektronického podpisu.

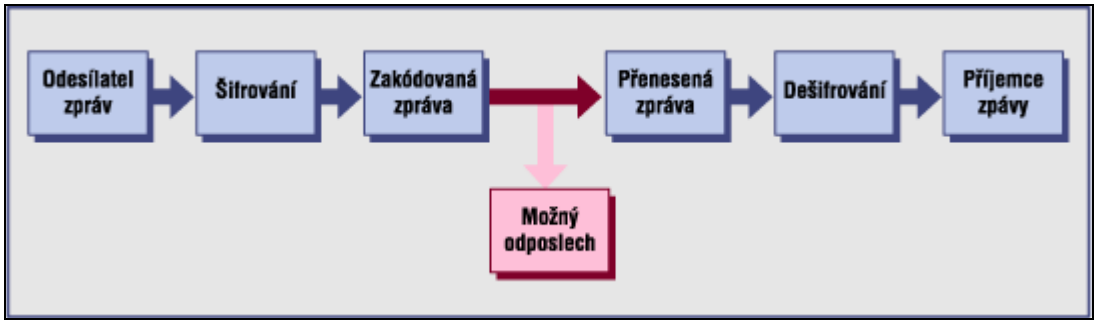
V návaznosti na tento zákon byla udělena bývalým ministerstvem informatiky a ministerstvem vnitra akreditace třem společnostem (stav v roce 2008), které jsou na jejím základě oprávněny tyto kvalifikované certifikáty vydávat. Jedná se o:

- **První certifikační autorita, a. s**.
  identifikační číslo 26 43 93 95,
  Podvinný mlýn 2178/6,
  PSČ 190 00 Praha 9
- **Česká pošta, s. p.**
  identifikační číslo 47 11 49 83,
  Olšanská 38/9,
  PSČ 225 99 Praha 3
- **eIdentity, a. s.**
  identifikační číslo 27 11 24 89,
  Vinohradská 184/2396,
  PSČ 130 00 Praha 3

Sdílení a výměna informací v elektronické podobě se v poslední době stává trendem. Ne každá informace je však určena komukoli, jinak řečeno, data je třeba chránit. Jedná-li se pak o elektronickou komunikaci ve sféře státní správy, zdravotnictví, financí apod. je více než nutné, aby byla stejně důvěryhodná jako klasické procedury prováděné prostřednictvím osobního styku, tedy zejména s využitím ověření totožnosti či vlastnoručního podpisu. *„Na základě této úvahy lze v souladu s mezinárodními normami definovat základní bezpečností cíle, jejichž plnění by měl důvěryhodný systém zajistit.“*[34] Jedná se především o zajištění důvěrnosti informací. Tzn., že musí být systémově zabezpečeno, aby přístup k důvěrným informacím měli pouze autorizované osoby. Dále musí být zajištěna integrita, tj. zabezpečení informací proti modifikaci, a neodmítnutelnost odpovědnosti. Pod neodmítnutelností odpovědnosti se skrývá schopnost a zároveň povinnost systému přesvědčit třetí nezávislou stranu o přímé odpovědnosti subjektu za autorství, případně za odeslání nebo přijetí zprávy.

4.2.3 Šifrování

Jednou z možností ochrany dat je šifrování neboli kryptografie.



Obrázek 5: Ukázka přenosu zpráv prostřednictvím šifrovacího kanálu.
Zdroj: www.ica.cz

Kryptografie je *„nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí.“*[35] Stupeň kvality ochrany zprávy je podmíněn použitou šifrovací metodou, typem užitého algoritmu, jeho aplikací a délkou šifrovacího klíče. V zásadě rozlišujeme šifrovací metody na metodu symetrické šifry a metodu asymetrické šifry.

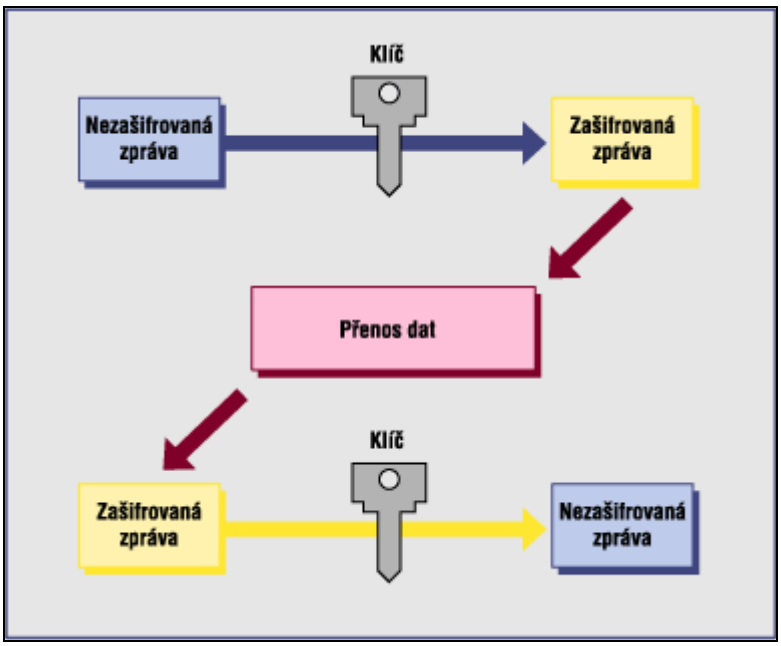
4.2.3.1 Symetrické šifry

Symetrická šifra je takový algoritmus, který k šifrování i dešifrování používá stejný klíč. Podstatnou výhodou těchto šifer je jejich nízká výpočetní náročnost. Na druhou stranu je tu

[34] Štědroň, B.: *Úvod do eGovernmentu*, Praha: Úřad vlády České republiky, 2007, str. 42
[35] Kryptografie. http://cs.wikipedia.org/wiki/Kryptografie, cit. [12. 4. 2008] online

ale nutnost sdílení tajného klíče, což je velkou nevýhodou. Odesílatel a příjemce šifrované zprávy se totiž musí předem domluvit na tajném klíči.

Symetrické šifry jsou obvykle užívány společně s asymetrickými. Použití je pak takové, že text je zašifrován symetrickou šifrou s náhodně vygenerovaným klíčem a tento klíč se následně zašifruje veřejným klíčem asymetrické šifry. Dešifrovat data pak může pouze majitel klíče asymetrické šifry. Dalším vhodným použitím, je zašifrování dokumentů, které se nikam neposílají, např. zašifrování dokumentu v počítači, aby ho nemohl otevřít nikdo nepovolaný.



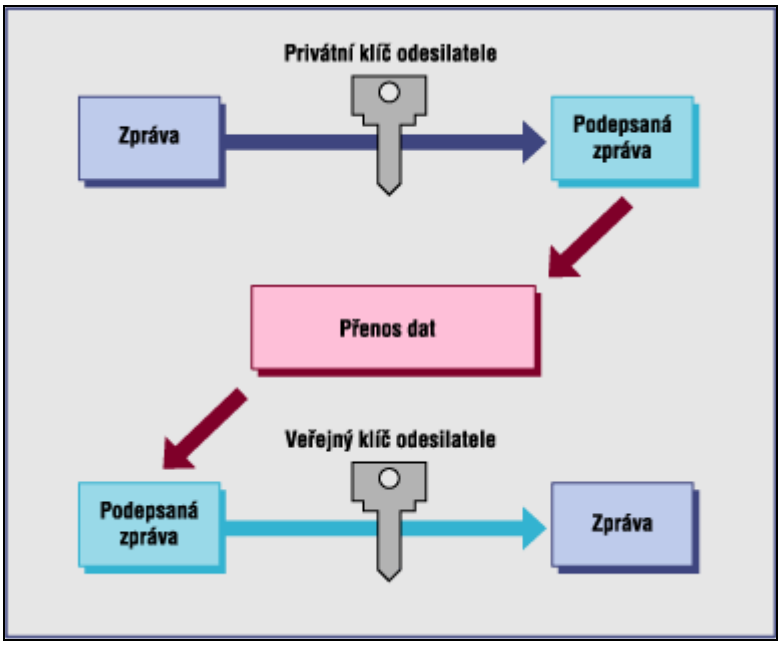
Obrázek 6: Ukázka symetrického šifrování.
Zdroj: www.ica.cz

4.2.3.2 Asymetrické šifry

Na rozdíl od symetrického šifrování využívá jednoznačně dané dvojice klíčů, jednoho na šifrování a druhého na dešifrování. Tuto dvojici klíčů si uživatel může vygenerovat za pomoci běžně dostupných softwarových produktů a stává se následně jejich jediným majitelem. *„Nejběžnější verzí asymetrické kryptografie je využívání tzv. veřejného a soukromého klíče“*[36] Soukromý klíč je bezpečně uložen u majitele (například na flash disku), zatímco druhý klíč je zveřejněný. Byla-li pak zpráva autorizována prostřednictvím soukromého klíče a my známe vlastníka veřejného klíče, za pomoci kterého jsme zprávu dešifrovali, známe odesílatele. Prostřednictvím takovéhoto využití asymetrické kryptografie lze řešit zabezpečení dat proti modifikaci a neodmítnutelnost odpovědnosti ze strany odesílatele. Pokud příjemce zašle i autorizované potvrzení o přijetí zprávy, bude zajištěna neodmítnutelnost odpovědnosti i ze

[36] Kryptografie. http://cs.wikipedia.org/wiki/Kryptografie, cit. [12. 4. 2008] online

strany příjemce. Tento postup ale neřeší požadavek na důvěrnost zpráv. K tomuto účelu je možné využít šifrování zpráv za pomoci veřejného klíče adresáta. Při tomto způsobu zašifrování máme jistotu, že tuto zprávu přečte jedině adresát se svým soukromým klíčem.



Obrázek 7: Ukázka asymetrického šifrování.
Zdroj: www.ica.cz

4.2.4 Možnosti praktického využití (e-podpis)

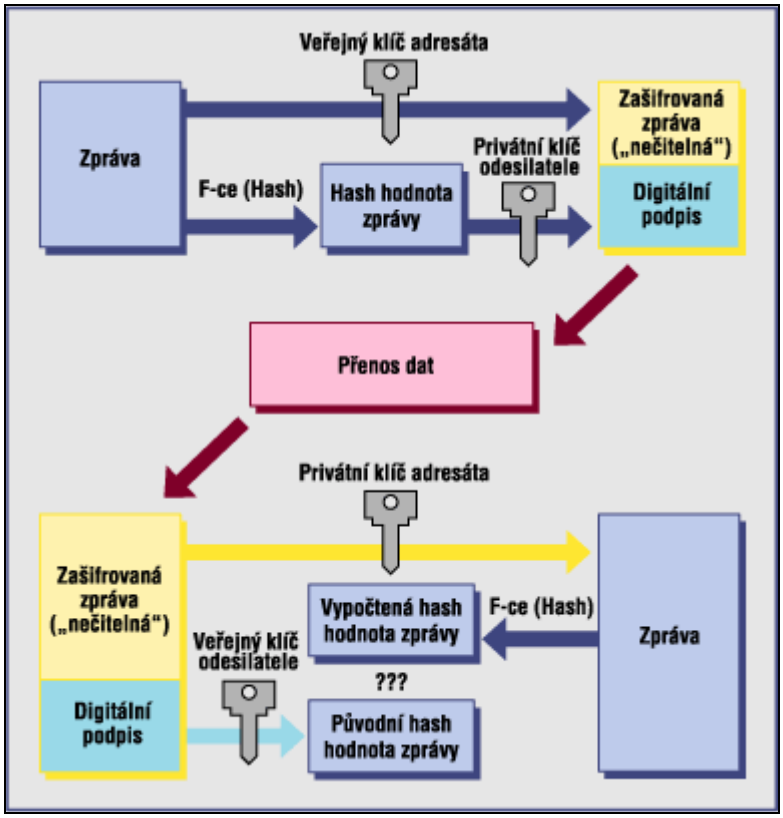
Aplikace asymetrických algoritmů je v porovnání s algoritmy symetrickými mnohem zdlouhavější. To je jeden z důvodů, proč se při tvorbě e-podpisu nešifruje privátním klíčem celá zpráva, ale nejprve se na data použije tzv. hash funkce. Hash funkce *„je reprodukovatelná metoda pro převod vstupních dat do (relativně) malého čísla, které vytváří jejich otisk (můžeme ho označit jako charakteristika dat)“*[37] tzv. Hash hodnotu. Opačný proces je nemožný, Hash funkce je totiž jednosměrná. Výpočet Hash hodnoty probíhá velmi rychle. Nejdříve se při podpisu zprávy vypočte její hash hodnota, která je o mnoho kratší než původní podepisovaná zpráva. Zpráva se šifruje asymetrickým algoritmem za použití soukromého klíče a výsledkem procesu je vytvoření tzv. elektronického podpisu. Ten se posléze odesílá jako příloha zprávy případně v samostatném bloku. Jeho výhodou je plnění stejných bezpečnostních kritérií jaké splňuje autorizace celého dokumentu, vytvoření elektronického podpisu však zabere nesrovnatelně méně času.

Ověření elektronického podpisu probíhá následovně:

- z datové zprávy je prostřednictvím hash funkce vytvořen kontrolní vzorek

[37]Hashovací funkce. http://cs.wikipedia.org/wiki/Hashovac%C3%AD_funkce, cit. [12. 4. 2008] online

- pomocí veřejného klíče podepisující osoby se dešifruje elektronický podpis a získá se tak kontrolní vzorek zprávy
- oba zjištěné vzorky se porovnají a v případě shody je pravost elektronického podpisu potvrzena



Obrázek 8: Ukázka zabezpečené komunikace
Zdroj: www.ica.cz

Primárním účelem elektronického podpisu je především zajištění nepopiratelnosti projevu vůle osoby, která se podepisuje vůči podepsané zprávě a zajištění integrity podepsané zprávy.

4.2.5 Certifikační autorita a certifikáty

Certifikační autorita se zabývá správou, distribucí a uchováním klíčů u jí vydaných produktů. Plní dvě funkce, validační (potvrzení platnosti certifikátu) a certifikační (zaručuje, že deklarovaný veřejný klíč patří dané osobě). Certifikační autorita má při komunikaci dvou subjektu funkci třetího nezávislého a důvěryhodného subjektu, který prostřednictvím jím vydaného certifikátu jednoznačně spojuje identifikace subjektu s jeho elektronickým podpisem. Certifikát se tak dá považovat za elektronický průkaz totožnosti. Certifikáty běžně obsahují veřejný klíč, jméno včetně dalších údajů zajišťujících nezaměnitelnost subjektu, datum počátku platnosti, datum ukončení platnosti a jméno certifikační autority, která certifikát vydala. Certifikační autorita je garantem jedinečnosti subjektů podle užité

identifikace subjektu. K zajištění slouží legislativní a technická pravidla provozu instituce certifikační autority. *„Splnění těchto požadavků potvrdí CA podpisem dokumentu svým privátním klíčem a následným vydáním tohoto certifikátu.“*[38]

Díky certifikačním autoritám se musí klient z hlediska ochrany utajovaných dat postarat pouze o bezpečné uchovávání svého soukromého klíče, protože ostatní je řešeno certifikáty. Existence certifikačních autorit také umožňuje důvěryhodnou komunikaci subjektů, které se vzájemně osobně nikdy nepotkali, případně těm kteří nechtějí podstupovat složitou proceduru důvěryhodné výměny svých klíčů.

4.2.5.1 Způsob získání a životní cyklus certifikátu

Pro zjednodušení je v následujícím textu uveden postup získávání kvalifikovaného certifikátu pro nepodnikající fyzickou osobu u České pošty.

Generování klíčů – každý zájemce o certifikát musí nejprve sám za pomoci dostupného softwaru vygenerovat dvojici klíčů pro použití v asymetrické kryptografii. U certifikátů vydávaných Českou poštou lze generování provést přímo na jejich stránkách[39], nutnou podmínkou je ale použití operačního systému Windows a prohlížeče Internet Explorer. Pokud nemá zájemce možnost využít online generování klíče, může provést generování prostřednictvím programu PostSignum Tool, který je volně ke stažení[40] .

Příprava podkladů – po vygenerování klíčů si musí zájemce připravit nutné podklady pro vydání certifikátu. Jedná se zejména stažení objednávky certifikačních služeb (vzor objednávky v příloze), o její vyplnění a vytištění ve dvou exemplářích. Následně si zvolíme typ certifikátu, který chceme využívat. Můžeme si vybrat kvalifikovaný certifikát pro ověření elektronického podpisu nepodnikající fyzické osoby nebo kvalifikovaný systémový certifikát pro ověření elektronické značky nepodnikající fyzické osoby. Po volbě následuje stažení zákaznického formuláře a jeho vyplnění podle přiložených vzorů.

Předání žádost na kontaktním místě – dalším krokem nutným k získání certifikátu, je navštívení kontaktního místa s požadovanými podklady. Těmito podklady jsou výše zmíněné dvě vytištěné objednávky certifikačních služeb, zákaznický formulář, vygenerovaná žádost o certifikát na disketě (v praxi je na některých pracovištích použitelný i flash disk) dva

[38] Štědroň, B.: *Úvod do eGovernmentu*, Praha: Úřad vlády České republiky, 2007, str. 50
[39] http://qca.postsignum.cz/www/generators.php
[40] http://qca.postsignum.cz/wizards/getpstool.php

doklady totožnosti (primárně občanský průkaz v kombinaci například s řidičským průkazem nebo pasem).

Kontrola informací – pracovník České pošty následně zkontroluje předloženou objednávku a zákaznický formulář. Pokud je vše v pořádku, jsou údaje zaneseny do systému, uzavřena smlouva a dojde k vystavení certifikátu.

Vydání certifikátu – pro samotné vydání certifikátu je třeba předložit výše uvedenou vygenerovanou žádost o certifikát na paměťovém médiu a dva doklady totožnosti. Po předložení podkladů je provedena kontrola totožnosti oproti dokladům a je provedeno vyhledání zájemcových údajů v systému PostSignum QCA. Pokud vše souhlasí, vytiskne se písemná žádost o certifikát a po jejím podpisu je certifikát vydán.

Na kontaktní místo se musí zájemce dostavit osobně, není možné zplnomocnění žádného zástupce nebo provést „dálkové“ vydání certifikátu.

Někteří poskytovatelé certifikačních služeb umožňují objednání testovacího certifikátů. Takovou službu nabízí konkrétně zmiňovaný První certifikační autorita a to na svých stránkách.

4.2.5.2 Platnost certifikátu

Doba platnosti vydaného certifikátu je omezená a je v každém certifikátu uvedena. Nejvyužívanější doba platnosti je v šest měsíců případně jeden rok. Tato omezená doba je hlavně z bezpečnostních důvodů, např. z důvodu možnosti vyzrazení privátního klíče. Certifikát lze majitelem zneplatnit i v průběhu platnosti a to buď na kontaktním místě certifikační autority a nebo žádostí o zneplatnění pomocí webu nebo e-mailu. K tomuto účelu je u certifikátu České pošty v písemné žádosti o certifikát doplněno heslo, které si zájemce sám zvolí.

5 Shrnutí

Rozšíření možností komunikace spojené s nástupem masového využívání internetu koncem 20. století znamenalo i rozvoj komunikace mezi orgány veřejné správy a občany. Zásadním zlomem byl hlavně rok 1999, kdy vznikla Státní informační politika ČR, první celostátní koncepce, která si vzala mimo jiné za cíl dosáhnou informační gramotností všech občanů, realizovat právo občana na přímý přístup k informacím nebo vybudovat komunikační infrastrukturu pro veřejnou správu.

Jeden ze základních kamenů úpravy elektronické komunikace s veřejnou správou je, Zákon o svobodném přístupu k informacím, který umožnil vyřizování žádostí o informace prostřednictvím elektronické pošty. Základní myšlenkou tohoto zákona je stanovení povinnosti orgánům veřejné správy, nezatajovat informace týkající se jejich činnosti a odpovědět na každý dotaz v zákonném termínu, případně sdělit zákonný důvod nemožnosti poskytnutí takové informace. Dalším pomyslným kamenem se o necelý rok později stal Zákon o elektronickém podpisu (2000), který ale prakticky začal platit až o rok a půl později, kdy byl vydán jeho prováděcí předpis. K rozvoji elektronizace veřejné sféry také přispěl vznik Úřadu pro veřejné informační systémy (2000), který byl zřízen jako ústřední správní úřad pro vytváření a rozvoj informačních systémů veřejné správy. Fungoval ale pouze tři roky a byl nahrazen Ministerstvem informatiky ČR, které po něm převzalo pomyslné žezlo v procesu elektronizace státu. Vznik ministerstva informatiky ale znamenal také významný odklon od původních ambiciózních strategických dokumentů přijatých v roce 1999. Ty byly totiž přehodnoceny a vše vyústilo ve schválení Státní informační a komunikační politiky, známé též pod názvem e-Česko. Jako členská země EU se Česká republika následně přihlásila i k aktualizovanému evropskému akčnímu plánu „eEurope 2005: Informační společnost pro všechny“. Bohužel je ale nutno říct, že řada cílů stanovených ve Státní informační a komunikační politice, nebyla ve svém termínu do roku 2006 splněna. Mám na mysli například cíl připravit legislativní úpravu pravidel pro výměnu dat mezi orgány veřejné správy a postavení základních registrů veřejné správy, která není upravena dodnes.

Elektronizace veřejné správy se spojuje s pojmem eGovernment. Rozvoj eGovernmentu v posledních letech značně zaostal oproti svému potenciálu, který byl vytvořen především vznikem dnes již bývalého ministerstva informatiky. Největším brzdou rozvoje eGovernmentu se jeví nedostatečná legislativní úprava, v některých případech dokonce její úplná absence. Současná absence legislativních úprav je zapříčiněna i faktem, že za dobu

existence ministerstva informatiky byl jeho zájem soustředěn především na zpřístupnění agend veřejné správy on-line. Konkrétní výsledkem této snahy je například Portál veřejné správy, který se především v prvním roce fungování ministerstva informatiky stal jeho „vlajkovou lodí“. Z důvodu absence jednotné legislativní úpravy dat, se ale z toho portálu stala pouze jakási nástěnka pro získávání informací z veřejné správy a o veřejné správě, pro kterou data musí být připravována v podstatě na zakázku. V současné době, co se týče podání, nabízí služby České správy sociálního zabezpečení, ministerstva průmyslu a obchodu, ministerstva financí, Generálního ředitelství cel, ministerstva dopravy a ministerstva životního prostředí.

Oblasti sdílení dat při výkonu veřejné moci, by se měl dotýkat návrh zákona ministerstva vnitra, tzv. zákon o eGovernmentu, který koncem března prošel prvním jednáním poslanecké sněmovny a jehož nabytí účinnosti je plánováno na 1. 7. 2009. Již v současnosti se ale ozývá řada hlasů s otázkou, zda právě forma, kterou tento návrh zákona v oblasti sdílení dat prezentuje, je tím nejšťastnějším řešením. Problém odpůrci vidí především v zabezpečení přístupu do jednotlivých registrů a s tím související možnost zneužití. Ochrana osobních údajů bude zajišťována elektronickým podpisem a systémem elektronické identity.

Kromě sdílení dat tento zákon mimo jiné zavádí povinnou formu elektronické komunikace mezi orgány veřejné moci a právnickými osobami prostřednictvím datových schránek nebo autorizovanou konverzí písemností, která by měla být nástrojem k omezení nutnosti předkládat některé dokumenty v písemné, ověřené podobě.

Zákon by se měl stát pomyslným srdcem projektu eGon, projektu ministerstva vnitra, který letos slaví své první narozeniny. Projekt je graficky znázorněn jako panáček eGon, který má čtyři části, prsty jeho rukou představují hustou kontaktní síť mezi úřady a občanem a tvoří je Czech POINTY. Oběhový systém představuje jednotnou komunikační infrastrukturu, srdce zákon o eGovernmentu (eGovernment act), a mozek je tvořen registry státní správy. Asi jedinou částí, která zatím v praxi funguje, jsou jeho prsty, Czech POINTY. Ty tvoří garantované služby pro komunikaci se státní správou prostřednictvím jednoho universálního místa. Na tomto místě lze získat ověřená data z informačních systému nebo ověření dokumentů a listin. Jedná se konkrétně o výpisy z Katastru nemovitostí, Obchodního rejstříku, Rejstříku trestů a z Živnostenského rejstříku. Počet těchto přístupových míst začal radikálně růst počátkem roku 2008, v současnosti tak lze Czech POINTY najít na cca 1600 různých místech v ČR i zahraničí.

Dalším zajímavým projektem je Virtuos, projekt Plzeňského kraje z 75 % financovaný z fondů EU, který má do budoucna ambice zahrnovat města a obecní úřady v celé české republice. Zatím se ale pouze rozbíhá a je do něj zapojeno pouhých 5 obecních úřadů.

Každoročně jsou prostřednictví různých soutěží oceňovány aktuální nejlepší projekty v oblasti elektronizace veřejné sféry. Mezi tyto soutěže patří například Zlatý erb vyhlašovaný, každoročně na konferenci ISSS a Egovernment The Best, který poslední dva roky pořádá magazín Egovernment. Prvně jmenovaná se soustřeďuje na hodnocení nejlepších webových stránek a elektronických služeb měst, obcí a krajů. Egovernment The Best se soustřeďuje na nejlepší projekty v daném roce. V letošním ročníku se nejlépe umístil již zmiňovaný Czech POINT, následovaný InfoSoudem a projektem přípravy materiálů v elektronické podobě pro jednání rady města a zastupitelstva města Uherského Brodu.

Elektronickou komunikaci je třeba zabezpečit. K tomu účelu je při komunikaci s veřejnou sférou ve většině případů nutné vlastnictví kvalifikovaného certifikátu, vydaného jednou ze tří autorizovaných certifikačních autorit. Opatřit zaručeným podpisem, který je založen na zmiňovaném kvalifikovaném certifikátu, je nutné například podání učiněné prostřednictvím e-podatelny.

6 Modelové situace

6.1 Elektronické podání daňového přiznání

6.1.1 Úvod

Existuje řada programů, které umožňují sestavení daňového přiznání v počítači. Jsou jimi například některé účetní programy, které tato přiznání vygenerují na základě informací z účetnictví automaticky. K tomuto účelu lze ale využít i programy, které nejsou přímo účetními programy, ale umožňují z takového účetního programu potřebných data načíst. Příkladem je program TaxEdit, který je spolupracuje s účetním programem Pohoda. Konkrétně v tomto programu je možné buď vyplněné daňové přiznání vytisknout a podat přímo, nebo vygenerovat elektronické podání ve formátu definovaném ministerstvem financí. Ukázku opisu elektronického potvrzení podání daňového přiznání učiněného prostřednictvím programu TaxEdit uvádím v příloze č. 2.

6.1.2 Ministerstvo financí

Ministerstvo financí nabízí možnost elektronického podání přímo na svých stránkách. Aplikace, jejímž prostřednictvím se toto přiznání podává, se jmenuje EPO. Tato aplikace má ale určitá softwarová omezení. Podle stránek ministerstva je k využívání této služby nutný počítač s operačním systémem Windows 2000, Windows XP nebo Knoppix verze 3.6. I přes ujištění, že aplikace podporuje i prohlížeč Mozilla Firefox nebo Opera, z vlastní zkušenosti doporučuji Internet Explorer.

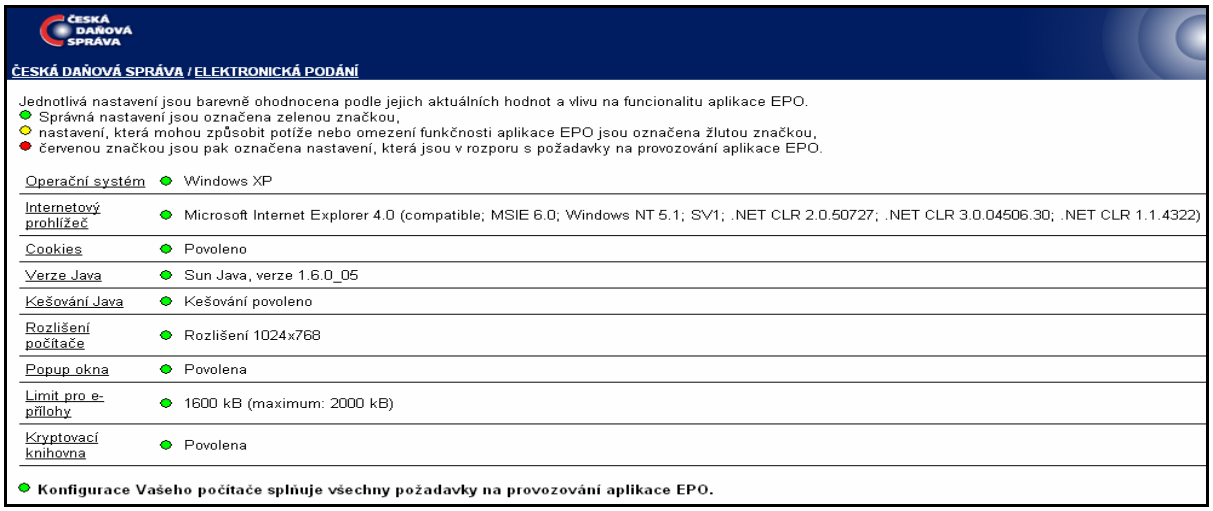
Druhou podmínkou pro podávání daňového přiznání elektronickou cestou je zaručený elektronický podpis založený na kvalifikovaném certifikátu.

EPO není nezbytně nutné používat přímo na internetu, je možné stažení do počítače a vyplnění přiznání tzv. off-line. Výsledný soubor se pak už jen načte do internetové verze aplikace a odešle.

Přístup ke zmiňované aplikaci EPO je možný buď prostřednictvím stránek ministerstva financí, nebo přes Portál veřejné správy. V dalším textu bych chtěl popsat podání prostřednictvím přístupu přes stránky ministerstva.

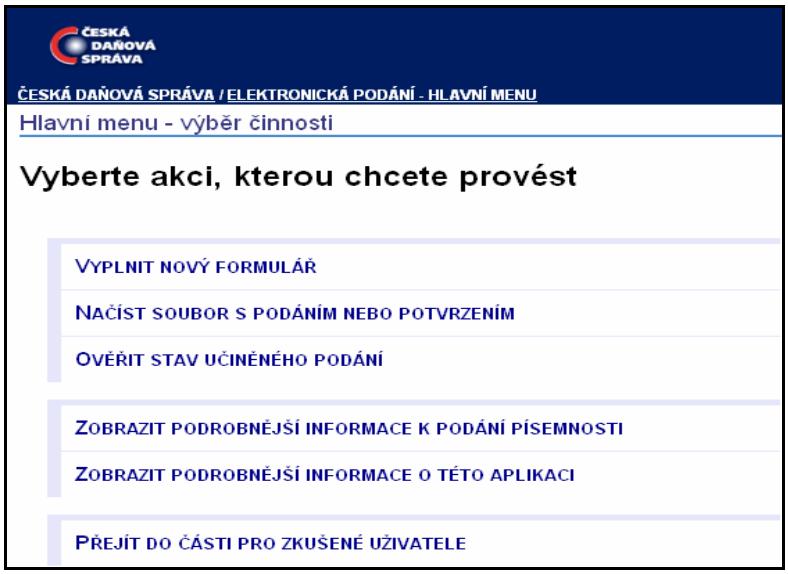
6.1.2.1 Postup podání

Na stránkách ministerstva financí[41] zvolíme v horní liště nabídku Daně a cla a následně v levé dolní liště nabídku EPO – el. podání. V okně, které se otevře, zvolíme položku Elektronické zpracování písemnosti. V dalším okně si můžeme otestovat, zda počítač splňuje podmínky aplikace, viz Obrázek 9, nebo přímo vstoupit do hlavního menu aplikace.



Obrázek 9: Test konfigurace počítače
Zdroj: www.mfcr.cz

V hlavním menu aplikace, viz Obrázek 10, si můžeme vybrat z nabídky vyplnění nového formuláře, načtení souboru s podáním nebo potvrzením, ověření stavu učiněného podání, zobrazení podrobnější informace k podání nebo zobrazení podrobnějších informací o aplikaci EPO.



Obrázek 10: Hlavní menu aplikace EPO
Zdroj: www.mfcr.cz

[41] www.mfcr.cz

Jako příklad jsem zvolil vyplnění nového formuláře přiznání k silniční dani. Jak je vidět v Obrázku 11, formulář přiznání k silniční dani se skládá ze záhlaví, I. oddílu, II. oddílu, zálohy, III. oddílu a přílohy.

Obrázek 11: Přiznání k silniční dani, záhlaví
Zdroj: www.mfcr.cz

Záhlaví

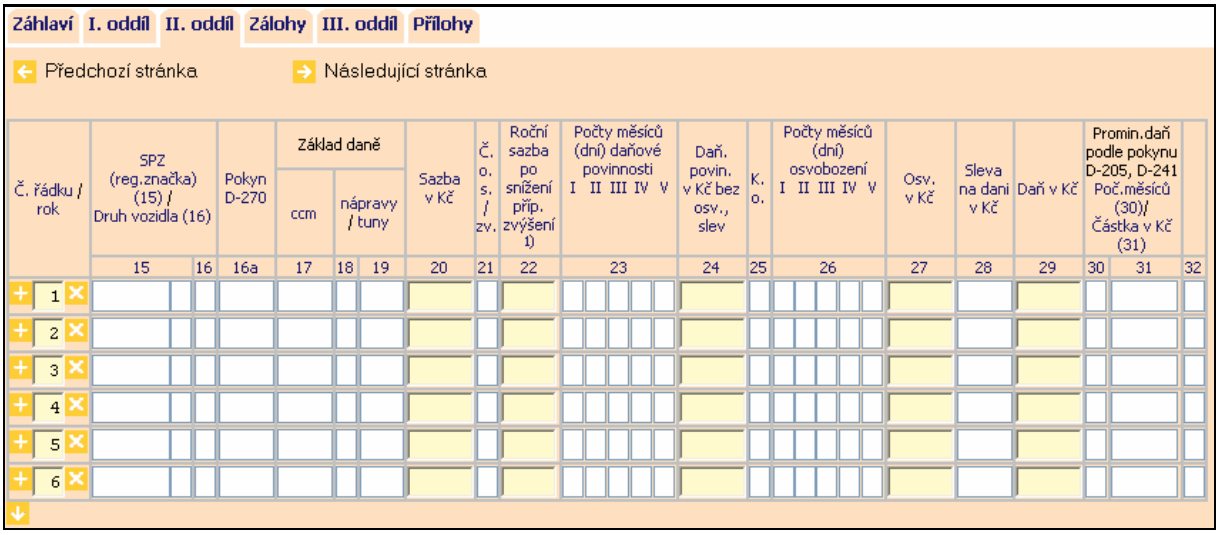
V záhlaví se vyplňuje finanční úřad, do jehož spádové oblasti podávající patří, DIČ, rodné číslo (IČO) a informace, zda je toto přiznání řádné, opravné nebo mimořádné.

I. oddíl

V I. oddílu jsou k vyplnění především údaje jako typ daňového subjektu, obchodní jméno právnické osoby, sídlo a případně údaje o daňovém poradci.

II. oddíl

Jak je vidět na Obrázku 12, tato část formuláře slouží k identifikaci automobilu, respektive automobilů, kterých se daň týká. Dále se v něm nachází k vyplnění informace o počtu měsíců daňové povinnosti, slev na dani apod. Po vyplnění těchto informací se automaticky vypočtou částky ve žlutých polích, tj. sazba v Kč, roční sazba po snížení nebo zvýšení, daň v Kč atd.



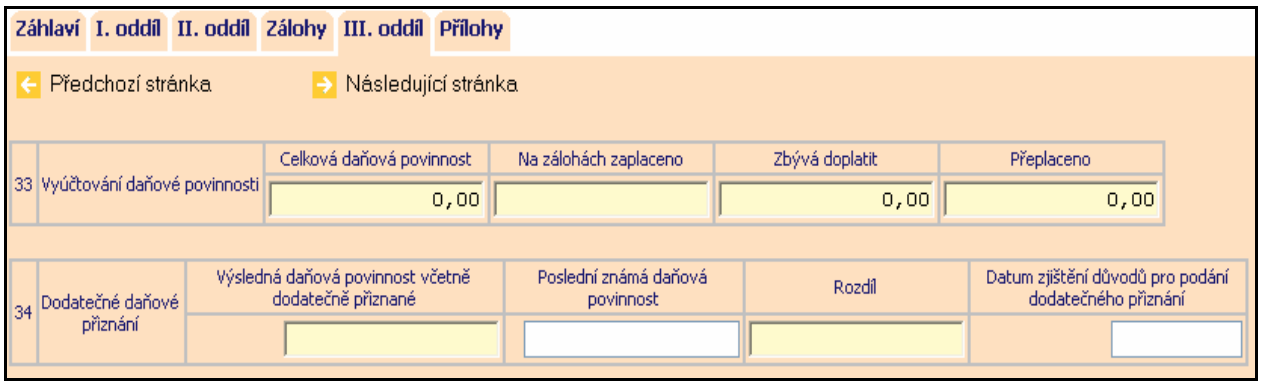
Obrázek 12: Přiznání k silniční dani, II. oddíl
Zdroj: www.mfcr.cz

Zálohy

U záloh jde o vyplnění data zaplacení zálohy a její částky.

III. oddíl

V této záložce se nacházejí souhrnné informace o celkové daňové povinnosti, o zaplacených zálohách a doplatku případně nedoplatku.



Obrázek 13: : Přiznání k silniční dani, III. oddíl
Zdroj: www.mfcr.cz

Přílohy

Záložka Přílohy nabízí možnost importu příloh v elektronické podobě. Aplikace EPO podporuje formáty DOC, XLS, PDF, JPG, TXT a RTF. Přiložené soubory tvoří nedílnou součást datové zprávy a v případě použití elektronického podpisu jsou podepsány společně s datovou správou.

6.1.2.2 Možnosti po vyplnění

Po vyplnění lze nechat přiznání překontrolovat, přepočítat, vytisknout, uložit k pozdějšímu vyvolání a nebo odeslat.

Po odeslání putuje formulář přes centrální evidenci k příslušnému finančnímu úřadu. Ten zkontroluje náležitosti tohoto přiznání a buď ho přijme nebo odmítne. O rozhodnutí je odesílatel informován prostřednictvím potvrzení, ve kterém jsou i přihlašovací údaje potřebné pro on-line sledování aktuálního stavu vyřízení podání.

6.1.3 Závěr

Proces podání přiznání se jejím prostřednictvím aplikace EPO velmi zjednodušuje a to i díky kvalitní nápovědě. Další pozitivní věcí je možnost uložení rozpracovaného podání do paměti počítače a možnost opětovného importu. I přes ujištění o podpoře jiných prohlížečů než je Internet Explorer, se mi v Mozille Firefox nepodařilo dané podání uskutečnit. Konkrétně jsem se dostal pouze do hlavního menu, kde mne systém upozornil, že vyplnění formuláře je možné pouze prostřednictvím Internet Explorer. Při využívání aplikace může zájemce narazit i na problém s vyskakujícími „popup“ okny. Konkrétně v mém počítači jsem musel nejdříve odinstalovat program ICQ toolbar, aby mi aplikace umožnila vyplnit formulář. Běžně nastavený počítač neprojde testem kompatibility, aniž by některá z testovaných částí alespoň „nezežloutla“, čili lehce nevyhovovala. Konkrétně podle tohoto testu nevyhovují ani fakultní počítače, ani počítač vedoucího práce.

6.2 Komunikace s orgány veřejné sféry

6.2.1 Úvod

Jak vyplývá z průzkumu studentů Fakulty managementu v zimním semestru 2007/2008, který byl realizován v rámci výuky, nejlépe a nejrychleji na elektronické dotazy odpovídají města. Relativně pohotové odpovědi se lze dočkat od některých Úřadů práce nebo např. od ministerstva financí. Další instituce, konkrétně ministerstvo vnitra, byly již méně pohotové, ale odpověď zaslaly alespoň v zákonném termínu, tj. do 30 dnů. Jak jsem se dozvěděl od vedoucího mé bakalářské práce, velmi špatně vyšly z dosud uskutečněných pokusů o získání

informací ministerstvo zdravotnictví a ministerstvo dopravy. Tyto ministerstva jsou v některých případech ochotna raději podstoupit riziko žaloby pro neposkytnutí informací na základě Zákona o svobodném přístupu k informacím, než by informace poskytla.

6.2.2 Městský úřad Ledeč nad Sázavou

Na základě těchto skutečností jsem si pro vyzkoušení fungování komunikace s orgány veřejné sféry vybral městský úřad, konkrétně v Ledči nad Sázavou. Dozvěděl jsem se, že město plánuje výstavbu plaveckého bazénu, a proto jsem na vybrané adresy odeslal e-mail v následujícím znění, obrázek 9.

Dobrý den,

zajímalo by mě, v jakém stádiu je plánovaná výstavba plaveckého bazénu v Ledči nad Sázavou. Konkrétně, jestli jsou v současnosti zajištěny finanční prostředky k realizaci daného projektu.

Děkuji

Pavel Buryánek

Obrázek 14: Dotaz

6.2.2.1 E-mail

První e-mail z dotazem jsem zaslal na adresu vedoucího odboru výstavby a životního prostřední Ing. Břetislava Dvořáka. Odpovědi se mi dostalo hned druhého dne ráno a to takové, že můj dotaz byl předán odboru samosprávy, konkrétně paní Čubanová, která má na starosti investice. O hodinu a půl později jsem obdržel e-mail od paní Čubanové, viz Obrázek 10.

Dobrý den,

K bazénu uvádím :

V současné době je vydáno územní rozhodnutí na „Sportovní centrum – přístavba bazénu a relaxačního centra" v Ledči nad Sázavou.
Čekáme až rozhodnutí nabude právní moci.
Poté půjde návrh do ZM, které musí rozhodnout o zadání PD.
Až bude vypracována PD můžeme teprve žádat o dotaci z EU.
Takže v současné době nevím, zda stihneme termín o podání dotace v září letošního roku.

S pozdravem
Čubanová

Obrázek 15: Odpověď od odboru samosprávy

Druhý e-mail jsem odeslal do kanceláře starosty, odpověď na Obrázku 11 jsem obdržel po dvou dnech.

Dobrý den,

na dostavbu sportovního centra o plavecký bazén a relaxační centrum máme zpracovanou dokumentaci pro územní řízení, které nyní probíhá, připravujeme se na podzimní výzvu ROPu, kdy chceme mít vyřízeno též stavební povolení. Do projektu bazénu jsme začlenili použití všech dostupných alternativních zdrojů energie (tepelná čerpadla, solární kolektory, rekuperace vzduchu, zpětné získávání tepla z chladících kompresorů) tak, abychom případné náklady na provoz bazénu a jeho energetickou náročnost snížili na minimum. Investiční náklady tím sice vzrostly, ale při předpokládané dotaci v řádu 80 – 90 % to je zanedbatelný nárůst. Z toho vyplývá, že finanční prostředky zatím zajištěny nemáme, chceme uspět s žádostí o získání prostředků z EU.

S pozdravem

Stanislav Vrba
Starosta města
Ledeč nad Sázavou
Mobil 731156911

Obrázek 16: Odpověď od kanceláře starosty

6.2.2.2 E-podatelna

Dotaz ve stejném znění jsem odeslal i na adresu elektronické podatelny. Jako reakce mi nepřišlo ani potvrzení o přijetí dotazu a ani odpověď. Přisuzuji to ale tomu, že dotaz nebyl podepsán kvalifikovaným podpisem a že úřad na můj dotaz již odpovídal prostřednictvím jiného komunikačního kanálu.

6.2.3 Závěr

Přesvědčil jsem se, že městské úřady komunikují velice dobře. Na vznesené e-mailové dotazy odpovídají prakticky bezprostředně a srozumitelně.

6.3 Vysoké školy

6.3.1 Úvod

Možnost podávat přihlášku ke studiu elektronicky v současnosti nabízí většina vysokých škol. Například Vysoká škola ekonomická v Praze, Univerzita Karlova, Univerzita Tomáše Bati ve Zlíně a Mendelova zemědělská a lesnická univerzita. Většinou je ale nutné doplnit toto elektronické podání o vytištěnou a podepsanou část přihlášky zaslanou poštou. Bohužel i zasílání výsledků elektronickou formou doplněnou certifikátem je stále budoucností.

6.3.2 Podání elektronické přihlášky ke studiu na VŠE

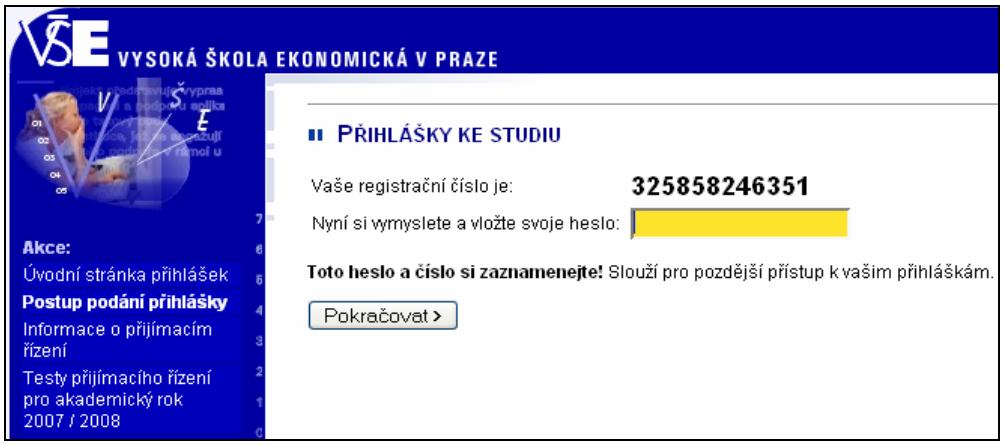
Jako jednu z modelových situací jsem zvolil podání elektronické přihlášky na Vysokou školu ekonomickou. Tuto přihlášku lze podat na centrálních stránkách VŠE, tedy na www.vse.cz.

6.3.2.1 Postup podání přihlášky

Krok 1.

Nejprve je nutné vyhledat web VŠE[42], vybrat nabídku přihlášky ke studiu a následně elektronické přihlášky ke studiu. V okně, které se zobrazí pak zvolíme nabídku Přidělit nové registrační číslo. Jak je vidět v následujícím obrázku, po těchto úkonech je uživateli přiděleno registrační číslo je vyzván k vložení jím zvoleného hesla.

Registrační číslo je nezbytné i při zjišťování výsledku přijímacího řízení na webu VŠE.



Obrázek 17: Přidělení registračního čísla a zvolení hesla
Zdroj: www.vse.cz

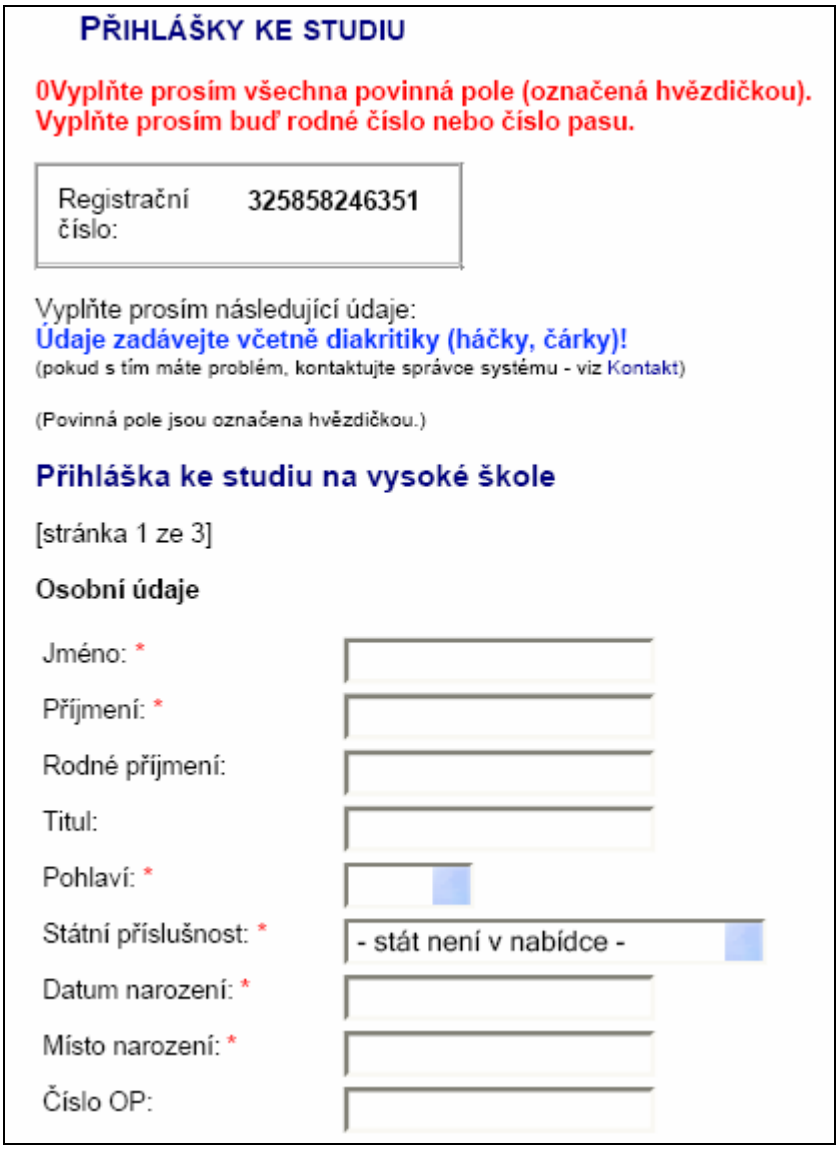
Krok 2.

Po vložení hesla se otevře okno, ve kterém se nacházejí další informace. Uživatel je mimo jiné upozorněn, že v akademickém roce 2008/2009 musí podat na každou fakultu přihlášku zvlášť a to pouze s výjimkou u Fakulty národohospodářské. Dále je informován, že nemá zatím žádné přihlášky a je mu nabídnuto vytvoření nové přihlášky.

[42] www.vse.cz

Krok 3.

Po odeslání požadavku o vytvoření nové přihlášky se zobrazí formulář přihlášky ke studiu. Část první strany toho formuláře zobrazuje obrázek 8.

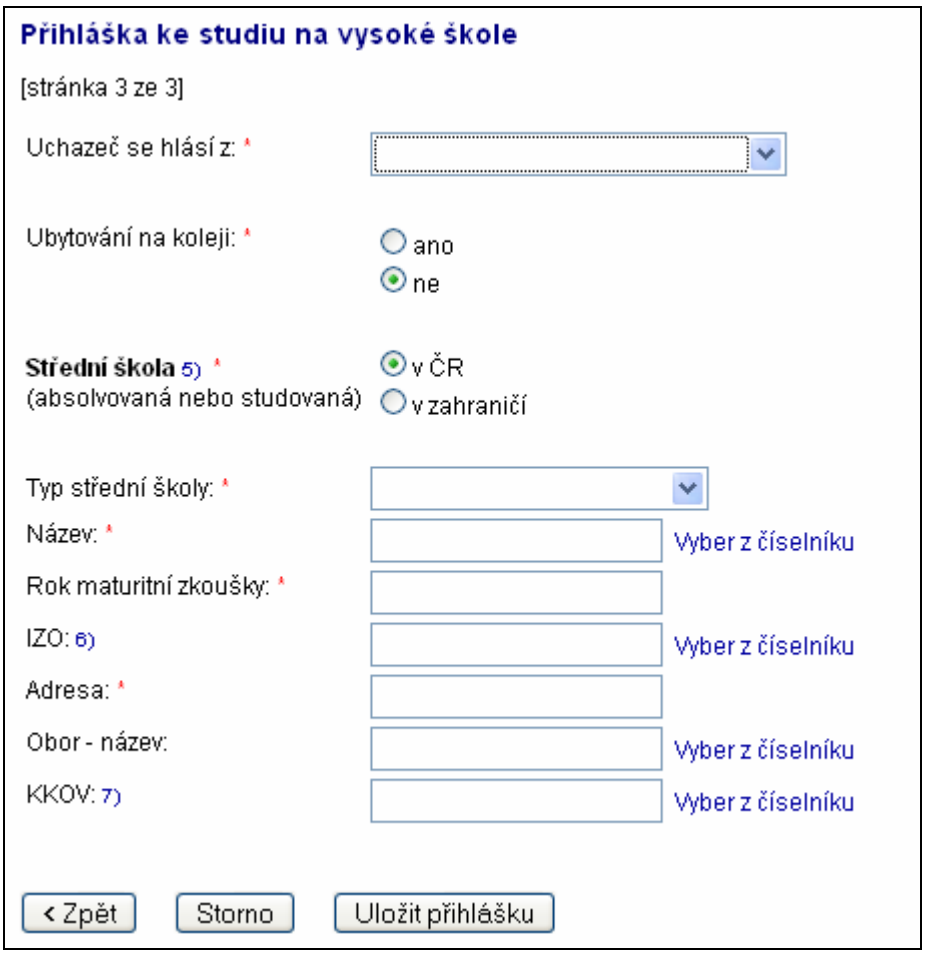


Obrázek 18: První strana přihlášky ke studiu
Zdroj: www.vse.cz

Na první straně formuláře jsou k vyplnění údaje o zájemci o studium. Kromě údajů zobrazených v předchozím obrázku jsou to ještě telefonní číslo a adresa.

Na druhé straně formuláře je k výběru typ studijního programu, akademický rok, forma studia, fakulta a studijní obor.

Na třetí straně, jak je vidět na Obrázku 8, jsou k vyplnění údaje o předchozím vzdělání. Po vyplnění těchto údajů přihlášku uložíme.



Obrázek 19: Třetí strana přihlášky ke studiu
Zdroj:www.vse.cz

Krok 4.

Po uložení přihlášky se zobrazí okno, Obrázek 9, ve kterém je možno zjistit stav přihlášky a případně tuto přihlášku ještě změnit nebo smazat. Pokud ani jednu z těchto možností nechceme využít, zvolíme uzavření přihlášky.

Obrázek 20: Závěrečná část vyplnění přihlášky
Zdroj: www.vse.cz

Krok 5.

Po uzavření přihlášky se údaj v kolonce Stav změní na „uzavřená“ a v kolonce Akce je pouze jediná možnost, vytisknout.

Pod tabulkou jsou zobrazeny pokyny, co dělat dál. Podle nich má zájemce přihlášku vytisknou, překontrolovat v ní obsažené údaje, podepsat a spolu s dokladem o zaplacení zaslat na poštovní adresu příslušné fakulty.

Po přijetí přihlášky a platby fakultou se v kolonce Stav objeví „přijatá“ a následně „zaplacená“.

6.3.3 Závěr

Systém podávání přihlášky hodnotím jako velmi dobrý. Bez problémů lze vyplnění provádět i v jiných prohlížečích než je Internet Explorer. Moje konkrétní zkušenost je s Mozillou Firefox. Vyplnění mimo jiné usnadňuje i možnost u charakterizování střední školy vybrat některé potřebné údaje z číselníku. Zaujala mě i možnost zjištění výsledku přijímacího řízení prostřednictvím přiděleného registračního čísla.

Možný potenciál toto elektronické podání ale bohužel nevyužívá. Nutí zájemce o studium k následnému vytištění, vlastnoručnímu podepsání a odeslání spolu s dokladem o zaplacení. Ověření identity prostřednictvím certifikátu je bohužel stále budoucností.

Závěr

Rozšíření možností komunikace spojené s nástupem masového využívání internetu koncem 20. století znamenalo i rozvoj komunikace mezi orgány veřejné správy a občany.

V první kapitole práce se zabývám mapováním vývoje elektronické komunikace uvnitř veřejné správy a mezi veřejnou sférou a občany. Jedná se o vývoj od roku 1999, kdy byly podle mého názoru učiněny první důležité legislativní kroky pro její umožnění. Těmito kroky myslím především vznik dokumentu „Státní informační politika ČR“, Zákona o svobodném přístupu k informacím a Zákona o elektronickém podpisu. Nejdůležitější roli v prvních letech vývoje mělo hrát Ministerstvo informatiky ČR, které vzniklo v roce 2003. To ale podle všeho nevyužilo svého potenciálu a výsledkem jeho činnosti jsou většinou jen solitérní projekty a nesplněné cíle, které si stanovilo.

Ve druhé kapitole jsem se zaměřil na eGovernment, pojem, pod kterým se skrývá proces elektronizace státu. Zabývám se v ní překážkami rozvoje elektronizace státu v letech 1999–2006, možnostmi přístupu občanů k eGovernmentu, tzv. zákonem o eGovernmentu a současnými postoji uživatelů internetu k pojmu eGovernment.

Jako největší překážku rozvoje vidím trvající absenci legislativních úprav, které by umožnily rozvoj online služeb. Jedná se například o zákonnou úpravu sdílení dat ve veřejné správě, o kterou se pokoušelo již ministerstvo informatiky. Dalším problémem je přístup administrativního aparátu, který i přes současné technologické možnosti mimo jiné stále preferuje papírovou formu dokumentů před elektronickou a tím některé úkony zbytečně komplikuje, prodlužuje a i prodražuje. Příkladem je i nedávný článek v Mf DNES[43], podle kterého je kvůli jednomu jednání Parlamentu ČR potištěno 7 tun papíru, což znamená náklady ve výši 2,2 milionu korun.

Další věcí, kterou zmiňuji ve druhé kapitole, je výzkum týkající se aktuálních postojů k eGovernmentu. Z tohoto výzkumu mimo jiné vyplynulo, že celých 57 % častých uživatelů internetu pojem eGovernment nikdy neslyšelo. Vzhledem k tomu, že proces elektronizace státu probíhá již řadu let, nevypovídá to především o práci naší vlády nic dobrého.

Ve třetí kapitole se zabývám aktuálními projekty v oblasti elektronizace veřejné sféry a soutěžemi, které tyto projekty posuzují. K popsání jsem si vybral projekty, které mě zaujaly. Jedná se o projekt Egon, Czech POINT, VIRTUOS a Portál veřejné sféry. Nejvíce z jmenovaných mě zaujal projekt Czech POINT, který podle mého názoru velkou měrou

[43] Mf DNES z 28. 4. 2008

přispívá ke zjednodušení komunikace s některými orgány veřejné správy. Postupem času se navíc rapidně zvyšuje počet jeho kontaktních míst, poskytovaných služeb a tím i jeho přínos.

Z řady soutěží, které hodnotí projekty týkající se elektronizace státu, se ve třetí kapitole zmiňuji o Zlatém erbu a zejména o Egovernment The Best. Egovernment The Best mě zaujal především z důvodu, že projekty jsou vybírány na základě tipů čtenářů magazínu Egovernment a následně posuzovány podle kritérií převzatých ze soutěže European eGovernment Awards.

Elektronickou komunikaci je třeba také určitým způsobem zabezpečit, proto jsem se ve čtvrté kapitole na tuto problematiku rozhodl zaměřit. K tomuto účelu slouží především symetrické a asymetrické šifrovaní a certifikáty. Vyzkoušel jsem podepisování e-mailů prostřednictvím testovacího certifikátu poskytovaného První certifikační autoritou.

Pátou kapitolu představuje shrnutí předchozích čtyř.

V poslední, šesté kapitole, testuji některé služby, které veřejná sféra nabízí. Jmenovitě se jedná o elektronické podání přiznání k silniční dani, e-mailové zaslání dotazu na městský úřad a podání elektronické přihlášky ke studiu na VŠE. Výsledky testování zmiňuji na konci jednotlivých podkapitol.

Elektronické podání daňového přiznání hodnotím i přes některé technické obtíže jako velmi dobré. Jako hlavní problém vidím orientaci této služby na software společnosti Microsoft. Zasláním e-mailového dotazu na městský úřad v Ledči nad Sázavou, jsem si potvrdil zkušenost studentů fakulty managementu, že městské úřady odpovídají na tyto dotazy velice pohotově a nemají při poskytování informací touto cestou žádný problém. Elektronické podání přihlášky na VŠE považuji za bezproblémové a jednoduché. Jediným zklamáním je pro mě absence možnosti využití certifikátů a z toho vyplývající nutnost vytištění a podepsaní vytvořené přihlášky.

Prakticky je elektronizace veřejné správy v České republice i přes některé snahy stále v počátcích a záleží jen na přístupu příštích vlád a úředníků, zda se tato situace nějak změní.

Literatura

[1] Štědroň, B.: *Úvod do eGovernmentu*, Praha: Úřad vlády České republiky, 2007, ISBN 978-80-87041-25-3

[2] Rybka, M., Malý, O.: *Jak komunikovat elektronicky*, Grada, 2002, ISBN 80-247-0208-8

[3] Mates, P., Smejkal, V.: *E-government v českém právu*, Linde Praha a.s., 2006, ISBN 80-7201-614-8

[4] Bitto, O.: *Šifrování a biometrika aneb Tajemné bity a dotyky*, Praha: Computer Media, 2005, ISBN 80-86686-48-5

[5] http://www.kr-vysocina.cz/

[6] http://www.mvcr.cz/

[7] http://www.wikipedia.cz/

[8] http://www.businessinfo.cz/

[9] http://www.egovernment.cz/

[10] http://www.langer.cz/

[11] http://www.elektrorevue.cz/

[12] http://vsol.obce.cz/

[13] http://www.fzu.cz/

[14] http://www.pgp.cz/

[15] http://qca.postsignum.cz/

[16] http://www.esfcr.cz/

[17] http://www.adaptic.cz/

[18] https://teta.fm.vse.cz/

[19] https://moodle.fm.vse.cz/

[20] http://moderniobec.ihned.cz/

[21] http://www.feedit.cz/

[22] http://www.isvs.cz/

[23] http://www.isss.cz

[24] http://www.mfcr.cz

[25] http://www.justice.cz

[26] http://www.infosoud.justice.cz

[27] http://www.ledecns.cz

[28] http://www.vse.cz

Seznam obrázků

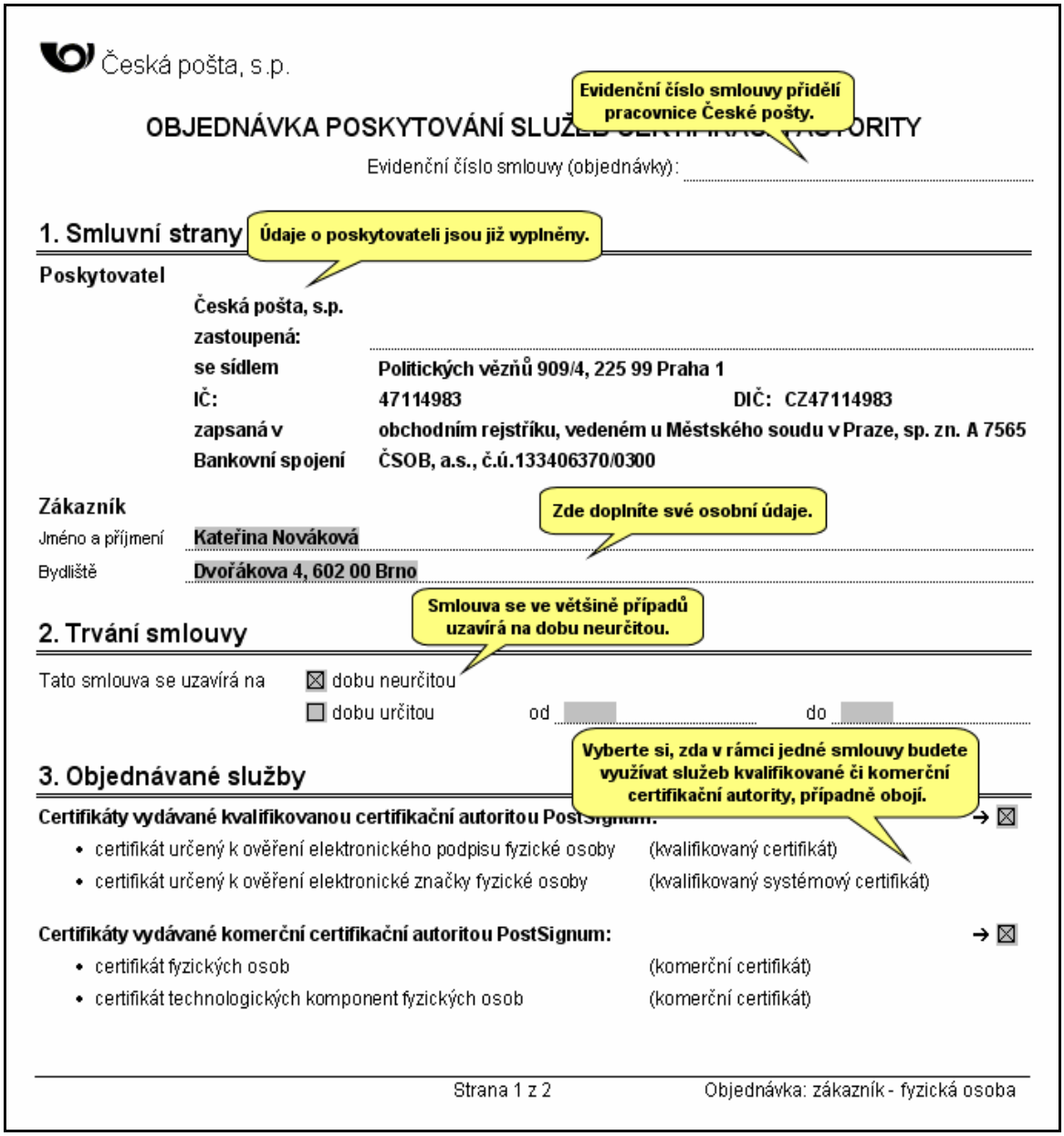
Seznam grafů

Seznam tabulek

Přílohy

Příloha č. 1
Příklad vyplněné objednávky na poskytování služeb certifikační autority, str. 1/2

Zdroj: http://qca.postsignum.cz



Česká pošta, s.p.

Evidenční číslo smlouvy přidělí pracovnice České pošty.

OBJEDNÁVKA POSKYTOVÁNÍ SLUŽEB CERTIFIKAČNÍ AUTORITY

Evidenční číslo smlouvy (objednávky): .....

1. Smluvní strany

Údaje o poskytovateli jsou již vyplněny.

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

Zde doplníte své osobní údaje.

Jméno a příjmení: Kateřina Nováková

Bydliště: Dvořákova 4, 602 00 Brno

2. Trvání smlouvy

Smlouva se ve většině případů uzavírá na dobu neurčitou.

Tato smlouva se uzavírá na ☒ dobu neurčitou

☐ dobu určitou od ..... do .....

3. Objednávané služby

Vyberte si, zda v rámci jedné smlouvy budete využívat služeb kvalifikované či komerční certifikační autority, případně obojí.

Certifikáty vydávané kvalifikovanou certifikační autoritou PostSignum: → ☒

- certifikát určený k ověření elektronického podpisu fyzické osoby (kvalifikovaný certifikát)
- certifikát určený k ověření elektronické značky fyzické osoby (kvalifikovaný systémový certifikát)

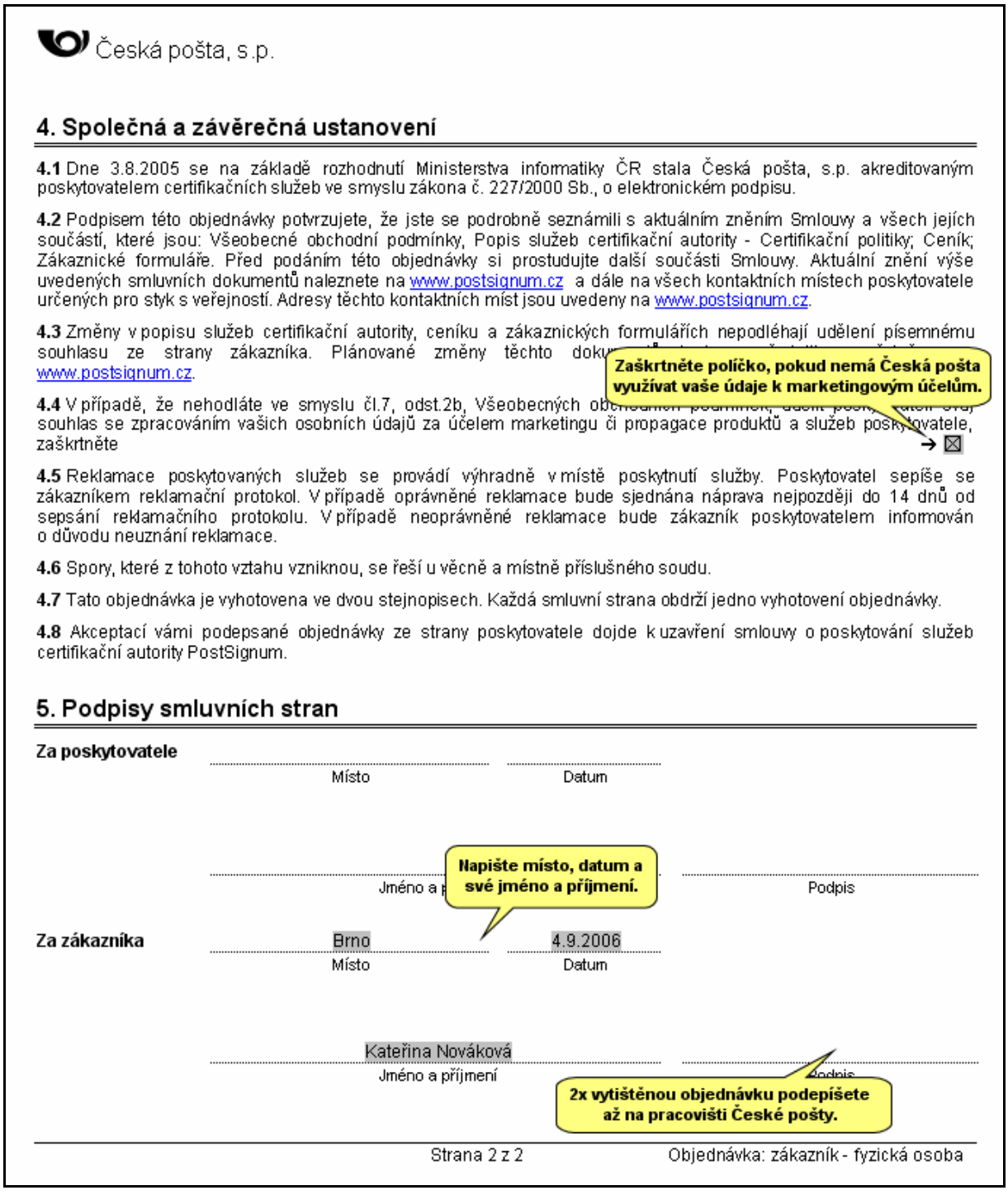
Certifikáty vydávané komerční certifikační autoritou PostSignum: → ☒

- certifikát fyzických osob (komerční certifikát)
- certifikát technologických komponent fyzických osob (komerční certifikát)

Strana 1 z 2 Objednávka: zákazník - fyzická osoba

Příklad vyplněné objednávky poskytování služeb certifikační autority str. 2/2.

Zdroj: http://qca.postsignum.cz



Česká pošta, s.p.

4. Společná a závěrečná ustanovení

4.1 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.

4.2 Podpisem této objednávky potvrzujete, že jste se podrobně seznámili s aktuálním zněním Smlouvy a všech jejích součástí, které jsou: Všeobecné obchodní podmínky, Popis služeb certifikační autority - Certifikační politiky; Ceník; Zákaznické formuláře. Před podáním této objednávky si prostudujte další součásti Smlouvy. Aktuální znění výše uvedených smluvních dokumentů naleznete na www.postsignum.cz a dále na všech kontaktních místech poskytovatele určených pro styk s veřejností. Adresy těchto kontaktních míst jsou uvedeny na www.postsignum.cz.

4.3 Změny v popisu služeb certifikační autority, ceníku a zákaznických formulářích nepodléhají udělení písemnému souhlasu ze strany zákazníka. Plánované změny těchto doku
www.postsignum.cz.

Zaškrtněte políčko, pokud nemá Česká pošta využívat vaše údaje k marketingovým účelům.

4.4 V případě, že nehodláte ve smyslu čl.7, odst.2b, Všeobecných ob
souhlas se zpracováním vašich osobních údajů za účelem marketingu či propagace produktů a služeb posky
zaškrtněte ☒

4.5 Reklamace poskytovaných služeb se provádí výhradně v místě poskytnutí služby. Poskytovatel sepíše se zákazníkem reklamační protokol. V případě oprávněné reklamace bude sjednána náprava nejpozději do 14 dnů od sepsání reklamačního protokolu. V případě neoprávněné reklamace bude zákazník poskytovatelem informován o důvodu neuznání reklamace.

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

4.7 Tato objednávka je vyhotovena ve dvou stejnopisech. Každá smluvní strana obdrží jedno vyhotovení objednávky.

4.8 Akceptací vámi podepsané objednávky ze strany poskytovatele dojde k uzavření smlouvy o poskytování služeb certifikační autority PostSignum.

5. Podpisy smluvních stran

Za poskytovatele

Místo ..... Datum .....

Jméno a p ..... Podpis .....

Napište místo, datum a své jméno a příjmení.

Za zákazníka

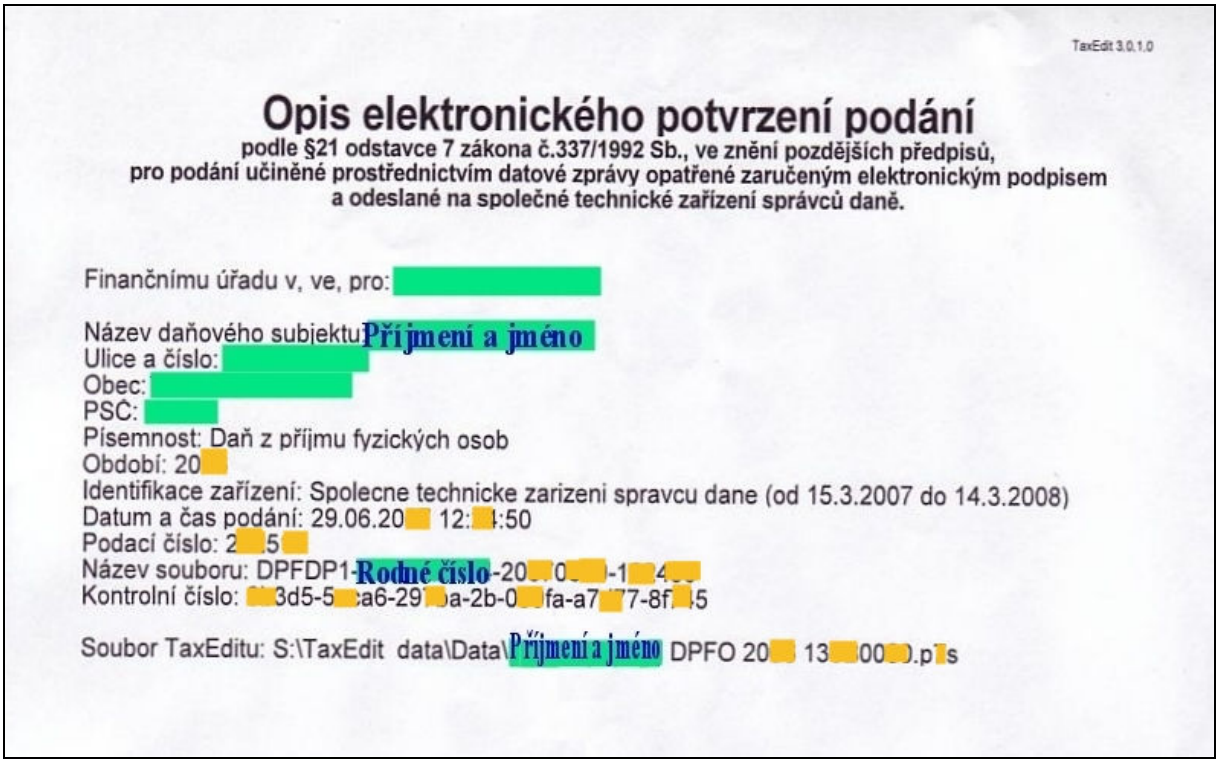
Brno (Místo) ..... 4.9.2006 (Datum) .....

Kateřina Nováková (Jméno a příjmení) .....

2x vytištěnou objednávku podepíšete až na pracovišti České pošty.

Příloha č. 2

Ukázka opisu elektronického potvrzení podání daňového přiznání učiněného prostřednictvím programu TaxEdit.



TaxEdit 3.0.1.0

Opis elektronického potvrzení podání

podle §21 odstavce 7 zákona č.337/1992 Sb., ve znění pozdějších předpisů, pro podání učiněné prostřednictvím datové zprávy opatřené zaručeným elektronickým podpisem a odeslané na společné technické zařízení správců daně.

Finančnímu úřadu v, ve, pro:

Název daňového subjektu Příjmení a jméno
Ulice a číslo:
Obec:
PSČ:
Písemnost: Daň z příjmu fyzických osob
Období: 20
Identifikace zařízení: Spolecne technicke zarizeni spravcu dane (od 15.3.2007 do 14.3.2008)
Datum a čas podání: 29.06.20 12: :50
Podací číslo: 2 5
Název souboru: DPFDP1-Rodné číslo-20 0 -1 4
Kontrolní číslo: 3d5-5 a6-29 a-2b-0 fa-a7 7-8f 5

Soubor TaxEditu: S:\TaxEdit data\Data\Příjmení a jméno DPFO 20 13 00 .p s