ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
PROVOZNĚ EKONOMICKÁ FAKULTA

Katedra informačních technologií

Bakalářská práce

Datové schránky:
Státní správa vs. komerční sféra

AUTOR: Miloslav Vrána

VEDOUCÍ PRÁCE: RNDr. Dagmar Brechlerová, Ph.D.

Česká zemědělská univerzita v Praze | Provozně ekonomická fakulta

Katedra informačních technologií | Akademický rok 2010/2011

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Miloslav Vrána

obor Veřejná správa a regionální rozvoj - Cheb

Vedoucí katedry Vám ve smyslu Studijního a zkušebního řádu ČZU v Praze čl. 16 určuje tuto bakalářskou práci.

Název práce: **Datové schránky: státní správa versus komerční sféra**

Osnova bakalářské práce:

1. Úvod
2. Cíl práce a metodika
3. Datové schránky a jejich využití ve státní správě
4. Výhody a nevýhody využití datových schránek ve státní správě
5. Datové schránky a jejich využití u právnických osob (v komerční sféře)
6. Výhody a nevýhody využití datových schránek u právnických osob (v komerční sféře)
7. Kvalita řešení, propagace, stav využití v roce 2010, Česká pošta, Ministerstvo vnitra
8. Závěr
9. Seznam použitých zdrojů
10. Přílohy

Rozsah hlavní textové části: 30 - 40 stran

Doporučené zdroje:

Smejkal V.,Datové schránky v právním řádu ČR,
978-80-86284-78-1,Rok vydání: 2009, Nakladatelství MJF

Lidinský V.,Švarcová I.,Budiš P., Loebl Z.,Procházková B., eGovernment bezpečně, 978-80-247-2462-1,Grada, 2008

Štědroň B., Úvod do eGovernmentu (Právní a technický průvodce),Praha: Úřad vlády české republiky, 2007. ISBN 978-80-87041-25-3.

Vedoucí bakalářské práce: **RNDr. Dagmar Brechlerová, Ph.D.**

Termín odevzdání bakalářské práce: březen 2011

.....
Vedoucí katedry

.....
Děkan

V Praze dne: 15. 3. 2011

Evidováno děkanátem PEF pod č.j.: KIT-293-10B

Prohlášení

Prohlašuji, že jsem bakalářskou práci *Datové schránky: Státní správa vs. komerční sféra* vypracoval samostatně pod vedením RNDr. Dagmar Brechlerové, Ph.D. a uvedl v seznamu literatury všechny použité literární a odborné zdroje. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Mariánských Lázních dne 25. Března 2011

_____

vlastnoruční podpis autora

Poděkování

Na tomto místě bych rád poděkoval RNDr. Dagmar Brechlerové, Ph.D. za cenné připomínky a odborné rady, kterými přispěla k vypracování této bakalářské práce.

Mariánské Lázně, březen 2011

Jméno a příjmení autora:	Miloslav Vrána
Název diplomové práce:	Datové schránky: Státní správa vs. komerční sféra
Název práce v angličtině:	Data Box: administration vs. sphere of business
Katedra:	Informačních technologií
Vedoucí bakalářské práce:	RNDr. Dagmar Brechlerová, Ph.D.
Rok obhajoby:	2011

Anotace

Tato práce popisuje zavádění datových schránek v rámci veřejné správy a samosprávy v České republice včetně zhodnocení efektivity provozu a vytýčení jednotlivých kladných i záporných stavů tohoto procesu.

Práce analyzuje zavádění datových schránek v rámci České republiky a na konkrétních příkladech popisuje tento proces. Upozorňuje na hlavní výhody a nevýhody datových schránek stejně tak, jako na problémy a aktuální překážky rozvoje eGovernmentu.

Annotation

Annotation

This work describes data boxes implementation in the frame of public administration and municipal government in the Czech Republic with the inclusion of performance effectivity evaluation and individual positive and negative stages of this process setting.

The work analysis data boxes implementation in the frame of the Czech Republic and describes this process on case studies. It also notices main advantages and disadvantages of data boxes as well as problems and actual obstructions of eGovernment development.

Klíčová slova

eGovernment, portál veřejné správy, datové schránky, e-volby, CzechPoint

Keywords

eGovernment, Portal of a Public Administration, Data Box, e-Voting, CzechPoint

OBSAH

1. ÚVOD

Osobně považuji zavedení eGovernmentu do státní správy za jeden z nejdůležitějších a klíčových bodů fungování vztahů mezi jednotlivými částmi státní správy a samosprávy, tak i ve vztahu k soukromé sféře. S ohledem na to, že se profesně věnuji oboru informačních technologií z pohledu poradenského již od roku 1993, usuzuji, že tento technologický milník je tématem, které je vhodné zmapovat, a i proto jsem si ho zvolil jako téma své bakalářské práce. Zavedení eGovernmentu lze považovat za důležitý strategický bod reformy veřejné správy. Tímto lze de facto poprvé konstatovat, že veřejná správa se mění takovým způsobem, že se začíná stávat občanům v této oblasti plnohodnotným partnerem v oblasti informačních technologií. Zavádění eGovernmentu navíc podporuje využití těchto procesů jako služby občanům a podnikatelům. A to tak, abychom mohli konstatovat začátek naplňování proklamovaného hesla: „ Obíhat mají dokumenty a ne občané.“

2. CÍL PRÁCE A METODIKA

Cílem práce je zmapování procesu zavádění datových schránek do státní správy, zhodnocení efektivity provozu a vytýčení jednotlivých kladných i záporných stavů tohoto procesu. Dále posouzení stavu, zda se státní správa z pohledu občana stává opravdu důvěryhodným partnerem, a to na všech úrovních a v co nejvíce životních situacích. Jedním z dalších dílčích cílů práce je posouzení provozního hlediska v oblasti snižování administrativních nákladů spojených s chodem veřejné správy.

Metodicky bylo v této práci postupováno analytickým způsobem s důrazem na využití vlastních zkušeností ze zprovozňování datových schránek na několika desítkách obecních a městských úřadů v ČR. Nejdříve byly vymezeny základní pojmy a zanalyzován stav od spuštění ostrého provozu v souladu se zadáním. Další část práce je věnována predikci vývoje eGovernmentu z pohledu vztahu státní správy, samosprávy, podnikatelského sektoru a občana.

3. REŠERŠE

Definice eGovernmentu dle OSN

„ Trvalá povinnost veřejné správy zlepšovat vztah mezi občany a veřejným sektorem poskytováním levných a efektivních služeb, informací a znalostí. Praktická realizace toho nejlepšího, co může veřejná správa nabídnout. “ (eGovernment bezpečně, Vít Lidinský a kol., 2008, str.7)

Tuto definici lze obecně považovat jako nejlépe vypovídající. Neřeší technickou část, ale jasně stanovuje cíl. Exaktně uvádí, že veřejná správa má nabízet občanům služby a to v té nejlepší možné míře

Definice eGovenrmentu dle MVČR

„ eGovernment představuje transformaci vnitřních a vnějších vztahů veřejné správy pomocí informačních a komunikačních technologií s cílem optimalizovat interní procesy. “ (eGovenrment bezpečně, Vít Lidinský a kol., 2008, str.7)

U definice publikované Ministerstvem vnitra jde především o zaměření se na strukturu veřejné správy a její optimalizaci. Není uváděno primárně že jde o službu, ale o proces, kterého výsledkem by nabídka služeb v nejlepší možné míře měla být.

prof.Ing.Vladimír Smejkal CSc. LL.M. Datové schránky v právním řádu ČR uvádí definici dle OECD, která jednoznačně určuje elektronickou komunikaci, prostřednictvím internetu, jako nástroj pro dosažení lepší správy. eGovernment si tedy lze odvodit jako nástroj, či provozování služby, která by měla přinášet zlepšení a ideální služby na straně uživatele i provozovatele. V tomto případě lze konstatovat, že občané mohou být na obou stranách, tedy jak provozovatelé, tak i uživatelé. Totéž lze konstatovat i o veřejné správě.

„ Zákon č. 300/2008 Sb. definuje datovou schránku jako elektronické úložiště, které je určeno k doručování orgány veřejné moci, provádění úkonů vůči orgánům veřejné moci a s účinností od 1. ledna 2010 (resp. v plném rozsahu od 1. července2010) též dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob (§ 2 odst. 1). Datové schránky zřizuje a spravuje Ministerstvo vnitra, to je také správcem informačního systému

datových schránek, který je informačním systémem veřejné správy obsahujícím informace o datových schránkách a jejich uživatelích. Provozovatelem tohoto informačního systému je držitel poštovní licence. Povinnosti Ministerstva vnitra jako správce informačního systému datových schránek a povinnosti provozovatele tohoto informačního systému vyplývají ze zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, a ze zákona č.300/2008 Sb. “

Zřizování datových schránek

a) ze zákona

Orgánům veřejné moci, právnickým osobám zřízeným zákonem, právnickým osobám zapsaným v obchodním rejstříku, organizačním složkám zahraničních právnických osob zapsaným v obchodním rejstříku a insolvenčním správcům byly datové schránky zřízeny ze zákona do 90 dnů od účinnosti zákona č. 300/2008 Sb. (tj. do 28. září 2009).

b) na žádost

Subjekty, jimž není datová schránka zřizována ze zákona, tj. fyzické osoby, většina podnikajících fyzických osob a část právnických osob (např. občanská sdružení, církve), mohou o zřízení datové schránky požádat. O zřízení další datové schránky mohou rovněž požádat orgány veřejné moci a právnické osoby, jejichž datová schránka právnické osoby plní současně funkci datové schránky orgánu veřejné moci.

Subjekty komunikace prostřednictvím datových schránek

Původní úprava obsažená v zákoně č. 300/2008 Sb. předpokládala využití komunikace prostřednictvím systému datových schránek mezi orgány veřejné moci navzájem a mezi orgány veřejné moci a fyzickými a právnickými osobami. Jednou ze stran komunikace měl být vždy orgán veřejné moci ve smyslu § 1 odst. 1 písm. a) zákona č. 300/2008 Sb. Novela zákona č. 300/2008 Sb. umožnila, aby od 1. ledna 2010, tj. po šesti měsících od nabytí účinnosti tohoto zákona, byly datové schránky užívány k dodávání datových zpráv i mezi soukromými subjekty.

Jedním z nejdůležitějších okamžiků a milníkem eGovernmentu je situace kdy „ Zavedením autorizované konverze dokumentů se tak v zásadě zrovnoprávňuje elektronická (digitální) a

listinná (analogová) podoba dokumentů při komunikaci s úřady.“ (Ministerstvo vnitra ČR Dostupné: ‚http://www.mvcr.cz/soubor/datove-schranky-dokumenty-datove-schranky-a-cinnost-spravnich-organu.aspx) [2011-03-21]

Okamžik zavedení autorizované konverze dokumentů lze v rozvoji eGovernmentu považovat za přelomový. Tradiční spojení a v myslích všech zakořeněné spojení, úředník – papír – razítko, ztrácí na významu. Zrovnoprávněním elektronické a listinné podoby dokumentů totiž ve své podstatě umožňuje především z legislativního hlediska používat elektronickou komunikaci v celé veřejné správě a taktéž i ve styku s občany a podnikateli.

„ Vzhledem k tomu, že podnikání je prováděno za účelem zisku, největší zisk budete mít z propojení velkých měst. Malé obce, které leží na geografických okrajích České republiky, míst s vysokou nadmořskou výškou a špatně přístupné lokality by se nevyplatilo připojovat. V případě, že by podnikatel připojení uvedených oblastí realizoval, by byla cena hovoru nebo datového přenosu astronomická. Vše je tedy regulováno tak, aby byly služby dostupné všem obyvatelům za jednotnou cenu. Princip solidarity je uplatněn tak, že geografická poloha bydliště neznevýhodňuje obyvatele v přístupu k těmto službám. Součástí telefonních služeb jsou ze zákona další činnosti, které nese poskytovatel jako „veřejně prospěšnou službu“. (eGovernment bezpečně, Vít Lidinský, a kol., 2008, str.29)

Otázkou zůstává, zda princip solidarity je uplatňován opravdu solidárně. Penetrace internetu již není v současné době tím hlavním problémem. Problémem je spíše cenová dostupnost této služby. Přední operátoři na trhu směřují své aktivity do rozvoje technologií, což sebou přináší nemalé náklady. I to je jeden z důvodů, proč cena internetového připojení v ČR nepatří z pohledu celého evropského telekomunikačního trhu mezi nejnižší. Masové rozšíření mezi 100% populace ochotné s internetem pracovat nás pravděpodobně v dohledné době z těchto důvodů nečeká.

JUDr. Bohumír Štědroň LL.M. uvádí, že „ Hlavními existujícími překážkami rozvoje eGovernmentu v letech 1999-2006 v České republice bylo:

1. Nemožnost sdílení dat mezi jednotlivými registry
2. Neexistence jediného bezvýznamného identifikátoru osoby

3. Nerovnoprávnost formy listinné s formou elektronickou
4. Nedostatečné vedení elektronických spisů a elektronické spisové služby

   (Úvod do eGovernmentu, JUDr. Bohumír Štědroň LL.M., 2007,str.30)

Elektronický podpis je jedním z nástrojů bezpečné elektronické komunikace. Nutnou podmínkou pro praktické využití elektronické komunikace je nastavení takových postupů, přístupů a principů, které bude možné považovat za rovnocenné běžné papírové agendě.

Na základě této úvahy lze v souladu s mezinárodními normami definovat základní bezpečnostní cíle, jejichž plnění by měl důvěryhodný komunikační systém zajistit:

- **důvěrnost informací** – systém musí zabezpečit, že přístup k důvěrným informacím mají pouze určené subjekty (osoby či systémy),
- **integrita** – systém musí zabezpečit informace proti modifikaci,
- **neodmítnutelnost** odpovědnosti – systém musí mít schopnost přesvědčit třetí nezávislou stranu o přímé odpovědnosti subjektu za autorství, vlastnictví, odeslání, případně přijetí zprávy.

  (eGovernment bezpečně, Vít Lidinský, a kol., 2008, str. 38)

Důvěrnost je možno definovat jako skutečnost, že data nebo informace nejsou předávány nebo prozrazovány neoprávněným stranám. Integritu jako skutečnost, že data nemohou být změněna. A neodmítnutelnost jako vlastnost, kdy pomocí kryptografických metod nelze popřít provedenou činnost. Přístup k důvěrným informacím v případě fyzické osoby, je možno definovat v celku bez problémů, protože podle § 13 odst.1 Obchodního Zákoníku, je-li podnikatelem fyzická osoba, jedná osobně nebo za ni jedná zástupce. V případě datových schránek je to administrátor nebo pověřená osoba. Je tedy jasné a srozumitelné, že v případě fyzické osoby je k přístupu oprávněna fyzická osoba, pro kterou byla datová schránka zřízena. Lze ale konstatovat, že oba autoři JUDr. Bohumír Štědroň LL.M. i Vít Lidinský ve svých publikacích shodně vymezili hlavní problémy eGovernmentu a liší se pouze technickými pojmy používanými v jednotlivých letech. Integrita jako pojem pro sdílení dat, důvěrnost informací jako neexistence identifikátoru osoby a neodmítnutelnost jako nerovnoprávnost

formy listinné s formou elektronickou. Jednotlivým problematickým okruhům jsou věnovány kapitoly 6 a 8.

„ K přístupu do datové schránky právnické osoby je oprávněn statutární orgán právnické osoby, člen statutárního orgánu právnické osoby nebo vedoucí organizační složky podniku zahraniční právnické osoby zapsané v obchodním rejstříku, pro něž byla datová schránka zřízena.“ (Datové schránky v právním řádu ČR, prof. Ing. Vladimír Smejkal, CSc. LL.M. 2009, str.57)

Zde je samozřejmě situace složitější. Statutárními orgány se myslí orgány, které byly za tímto účelem vytvořeny již ve zřizovacích dokumentech, a jež jsou oprávněny jednat ve všech věcech týkajících se právnické osoby. Kdo je statutární orgán právnické osoby, vyplývá tedy jednak z dikce platných zákonů, jednak z dalších dokumentů (zakladatelská listina, zápis z valné hromady, rozhodnutí jediného společníka apod.), případně ze zápisu v některém z rejstříků, přičemž tyto zápisy mohou mít charakter konstitutivní (vznik a zrušení společnosti), některé deklaratorní (změna jednatele).

„ Zákon rozeznává statutární orgány individuální a kolektivní, přičemž v tomto případě musí být stanoveno, jakým způsobem bude statutární orgán jednat. Právní úkony učiněné relevantním způsobem statutárním orgánem jsou přímo přičitatelné právnické osobě. V důsledku určitých právních skutečností může působnost statutárního orgánu částečně nebo zcela přejít také na jinou osobu (například na likvidátora či na správce konkurzní podstaty, resp. insolventního správce, nuceného správce apod.)“ (Datové schránky v právním řádu ČR, prof. Ing. Vladimír Smejkal, CSc. LL.M. 2009, str.57)

Z tohoto pohledu se dá konstatovat, že například, pokud chce zaměstnanec Czech Pointu doložit výpisem z obchodního rejstříku zapsání nového statutárního orgánu, tak to není možné. Nový statutární orgán potřebuje zpřístupnit datovou schránku proto, aby byl schopen podat návrh na změnu zápisu v obchodním rejstříku.

„ Legislativa umožňuje převedení informací obsažených v příslušných dokumentech do elektronické formy a uchování pouze elektronických dokumentů, pokud jsou splněny následující podmínky:

- informace jsou v písemné formě,

- jedná se o autentický dokument, resp. originál,
- je možné určit původce datové zprávy a datum a čas, kdy byla datová zpráva odeslána nebo doručena a
- požadavek úschovy se netýká informací, jejichž jediným účelem je komunikace příslušné informace.“

(eGovernment bezpečně, Vít Lidinský, a kol., 2008, str.74)

„ Zákon hovoří o tzv. autorizované konverzi, což znamená „úplné převedení dokumentu v listinné podobě do dokumentu obsaženého v datové zprávě, ověření shody obsahu těchto dokumentů a připojení ověřovací doložky“, nebo opačný směr konverze. Oba uvedené dokumenty mají shodné právní účinky.“ (eGovernment bezpečně, Vít Lidinský, a kol., 2008, str.74)

„ Z oblasti veřejné správy jsou bezpečnostní prvky zakotveny v právních předpisech upravujících následující oblasti:

- ochrana utajovaných informací,
- elektronické nástroje pro elektronické veřejné zakázky a
- informační systémy veřejné správy

V případě informačních systémů je většina zákonných požadavků věnována bezpečnostní dokumentaci. Tyto jsou zcela oprávněné, jelikož stanovit konkrétní opatření v rámci bezpečnosti není možné. Vzhledem k různorodosti informačních systémů a k rozsahu jejich činnosti je nutné bezpečnostní opatření definovat až na základě analýzy rizik. Konkrétní postupy a kroky při zajištění bezpečnosti informačního systému je možné převzít například ze zahraničních norem uvedených v legislativě.

V oblasti informačních a komunikačních technologií se dnes řeší:

- rozdílné nástroje pro správu zabezpečení,

- nejasný a nekonkrétní přehled o bezpečnostním stavu stanic, serverů a infrastruktury informačního systému,
- nedostatek informací o aktuálních bezpečnostních konfiguracích jednotlivých stanic a serverů,
- reakce různých dodavatelů na nové slabiny,
- vysoké zatížení stanic a serverů při zprovoznění bezpečnostních testů nebo aplikací bezpečnostních politik,
- integrace bezpečnostních komponent do stávající infrastruktury informačních systémů.“

(eGovernment bezpečně, Vít Lidinský, a kol.,2008, str.104)

Datové schránky a jejich právní úpravy ve světě

„ Základní úprava právních otázek spojených s eGovernmentem se datuje do roku 1996, jedná se o **UNCITRAL Model Law on Electronic Commerce** (dále jen „UNCITRAL Model Law“). http://www.uncitral.org/uncitral/en/index.html [2011-03-21] Tento modelový zákon je od doby svého vzniku inspirací pro nejrozvinutější státy světa při přípravě národní legislativy a vychází z něj např.i Evropská komise při přípravě evropské legislativy řešící některé aspekty elektronické komunikace. UNCITRAL Model Law vychází ve své úpravě z důsledného technologicky neutrálního přístupu a z rozlišení pojmu „písemnost“, „originál“, „podpis“, „úřední/notářské ověření“, „právní účinek/důkazní síla“ a „archivace dokumentů“.“ (eGovernment bezpečně, Vít Lidinský, a kol., 2008, str.104)

eGovernment v USA

„ V USA v roce 1999 vypracovali americkou obdobu UNCITRAL Model Law, tzv. Uniform Electrnic Transactions Act(1999). Tento návrh zákona vypracovala National Conference of Commissioners of Uniform State Laws, která připravuje unifikované zákony pro jednotlivé státy USA. V mezidobí tento zákon přijala naprostá většina států USA. V roce 2000 byl přijat federální zákon o elektronickém podpisu, tzv. E-Sign Act. Oba právní dokumenty vycházejí v podstatné míře z UNICTRAL Model Law, tento právní model však dále rozvíjejí. Oba

legislativní texty představují v současné době pravděpodobně nejmodernější právní úpravu elektronických obchodních transakcí uznávanou mezi odborníky na celém světě.“ (eGovernment bezpečně, Vít Lidinský, a kol., 2008, str.122)

eGovernment ve Velké Británii

„ Velká Británie dosáhla obdobného právního stavu jako USA, nikoliv však na základě zvláštních zákonů, ale zejména na základě soudních rozhodnutí. Anglické právo prakticky zrušilo požadavek na originál dokumentů. Ve Velké Británii byla rovněž vydána první soudní rozhodnutí, která přiznala plný právní účinek a důkazní sílu elektronickým dokumentům. Tato rozhodnutí sledovala obdobné požadavky, jaké jsou obsaženy v UNICTRAL Model Law.“ (eGovernment bezpečně, Vít Lidinský a kol., 2008, str.123)

eGovernment ve Finsku

„ Od roku 2004 běží ve Finsku projekt SÄHKE v pilotní formě. Cílem projektu SÄHKE je mimo jiné zkoumat, jak zajistit právní hodnotu elektronicky archivovaných dokumentů včetně stanovení požadavků týkajících se integrity a autenticity archivovaných záznamů. Národní archivy musí udělit povolení, aby dokumenty mohly být archivovány trvale pouze v elektronické formě.“ (eGovernment bezpečně, Vít Lidinský, a kol., 2008, str.129)

eGovernment ve Švédsku

„Právní rámec úpravy týkající se státních a úředních záznamů sestává z Freedom of the Press Act, Archives Act 1990, Secrecy Act, Data Act a prováděcích předpisů, převážně Archive Ordinance 1991, který zmocňuje Národní archivy (SNA)k vydání instrukcí týkajících se dokumentů veřejnoprávních institucí. Archives Act stanovuje, které státní úřady jsou odpovědným dohlížitelem na elektronické dokumenty.“ (eGovernment bezpečně, Vít Lidinský, a kol., 2008, str.132)

4. DATOVÉ SCHRÁNKY A JEJICH VYUŽITÍ VE STÁTNÍ SPRÁVĚ

Lze konstatovat, že za reálný začátek e-Governmentu můžeme považovat český státní projekt Czech POINT, v jehož rámci obecní úřady ORP, krajské úřady, notáři a další právnické osoby vydávají lidem výpisy z katastru nemovitostí, z rejstříku trestů či živnostenského rejstříku. Projekt vznikl 22. června 2005 a byl spuštěn v 37 obcí v roce 2007. Pracoviště Czech POINT jsou v současné době rozšířeny na více než 4500 obecních a krajských úřadech, vybraných pracovištích České pošty, zastupitelských úřadech, kancelářích Hospodářské komory a také v kancelářích notářů.

Nejdříve si rozčleňme jednotlivé okruhy, kterých se tato práce týká Těmito okruhy bude samotná státní správa a samospráva, dále právnické osoby a na závěr okruh stav a funkčnost dle plánovaných milníků při zavádění eGovernmentu v ČR. Lze tedy říci, že existují 3 základní typy komunikačních kanálů veřejné správy:

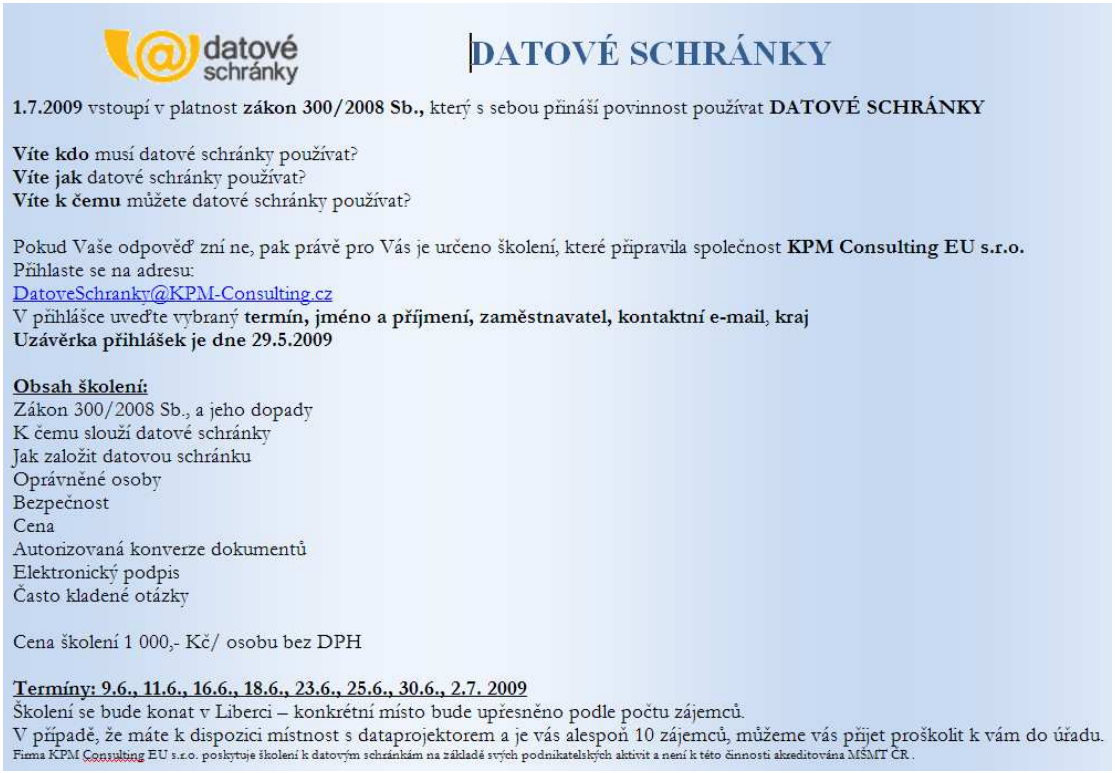
1. Komunikace státní správa (samospráva) – státní správa (samospráva)
2. Komunikace úřad – občan
3. e-Government - celková elektronizace veřejné správy obsažené v bodech 1 a 2

Komunikace úřad – úřad
Pro tuto situaci neposuzujeme, zda se jedná o komunikaci veřejné/státní správy či samosprávy, ale posuzujeme komunikaci obecně mezi všemi subjekty.

5. ANALÝZA ZAVÁDĚNÍ A SPOUŠTĚNÍ DATOVÝCH SCHRÁNEK VE STÁTNÍ SPRÁVĚ

Jako majitel soukromé firmy, která se zabývá poradenstvím v oblasti informačních technologií , jsem se rozhodl, v době, kdy se zprovozňovaly datové schránky, oslovit menší obce s nabídkou školení. A to na témata: „Jak založit datovou schránku“ a „ Jak používat datovou schránku“.

Informoval jsem se na Ministerstvu vnitra o tom, zda tato nabídka této služby není v rozporu se zákonem o datových schránkách a zda tuto službu mohu poskytovat bez akreditace. V obou případech mi bylo písemně sděleno, že nic z výše uvedeného není nutné. Nabídku školení jsem rozeslal emailem s podtextem, že má firma není akreditována pro školení datových schránek a veškeré informace a podklady poskytuje jako soukromoprávní subjekt.



datové schránky

DATOVÉ SCHRÁNKY

1.7.2009 vstoupí v platnost **zákon 300/2008 Sb.,** který s sebou přináší povinnost používat **DATOVÉ SCHRÁNKY**

Víte kdo musí datové schránky používat?
Víte jak datové schránky používat?
Víte k čemu můžete datové schránky používat?

Pokud Vaše odpověď zní ne, pak právě pro Vás je určeno školení, které připravila společnost **KPM Consulting EU s.r.o.**
Přihlaste se na adresu:
DatoveSchranky@KPM-Consulting.cz
V přihlášce uveďte vybraný **termín, jméno a příjmení, zaměstnavatel, kontaktní e-mail, kraj**
Uzávěrka přihlášek je dne 29.5.2009

Obsah školení:
Zákon 300/2008 Sb., a jeho dopady
K čemu slouží datové schránky
Jak založit datovou schránku
Oprávněné osoby
Bezpečnost
Cena
Autorizovaná konverze dokumentů
Elektronický podpis
Často kladené otázky

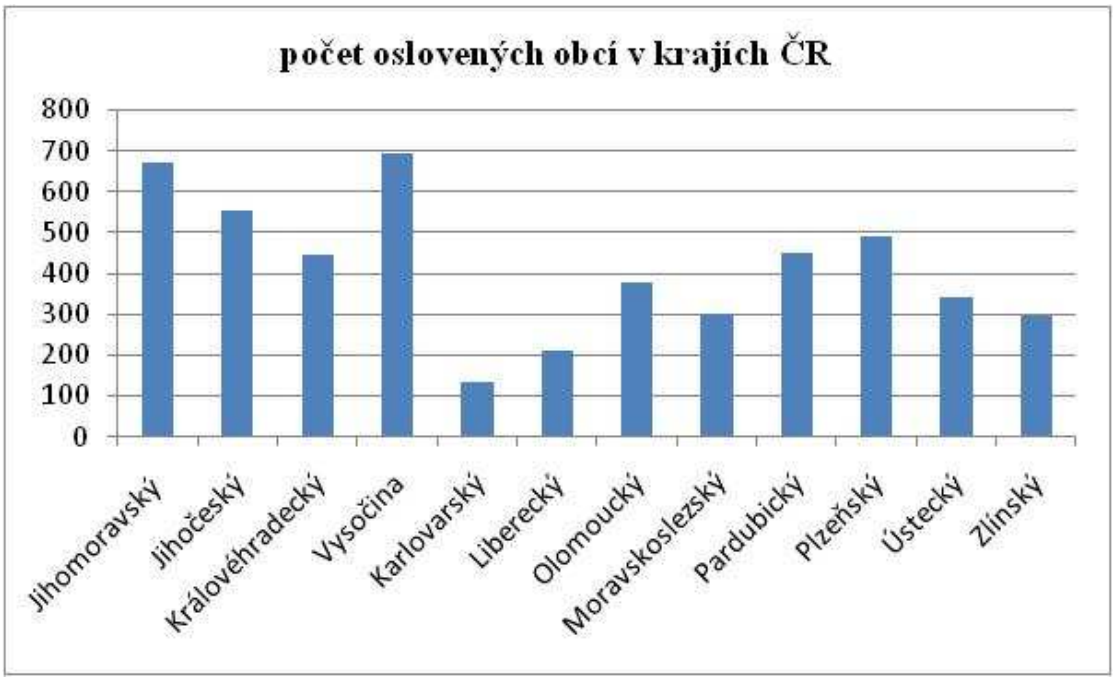
Cena školení 1 000,- Kč/ osobu bez DPH

Termíny: 9.6., 11.6., 16.6., 18.6., 23.6., 25.6., 30.6., 2.7. 2009
Školení se bude konat v Liberci – konkrétní místo bude upřesněno podle počtu zájemců.
V případě, že máte k dispozici místnost s dataprojektorem a je vás alespoň 10 zájemců, můžeme vás přijet proškolit k vám do úřadu.
Firma KPM Consulting EU s.r.o. poskytuje školení k datovým schránkám na základě svých podnikatelských aktivit a není k této činnosti akreditována MŠMT ČR.

Zdroj: zpracováno z informací poskytnutých firmou KPM Consulting EU s.r.o.

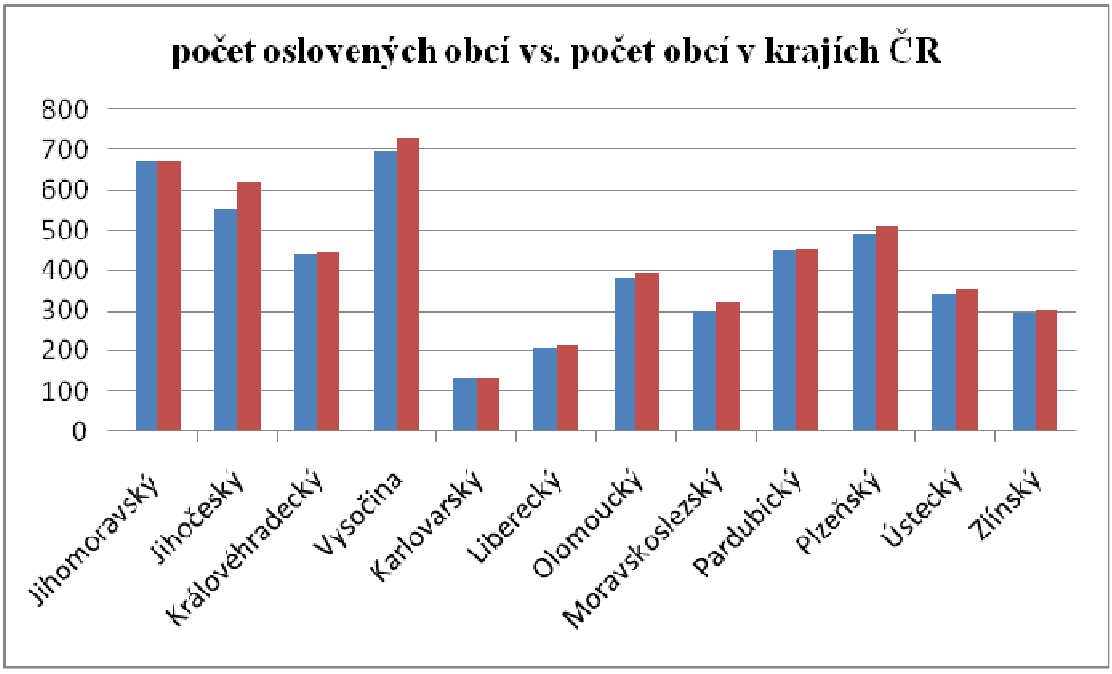
Bylo osloveno 13 krajů a v těchto 12 krajích celkem 4.965 obcí. Středočeský kraj a Praha byly jako lokality z oslovení vyjmuty z důvodů vysoké penetrace podobně odborně zaměřených firem.

Graf č.1 Počet oslovených obcí v jednotlivých krajích ČR



Ve srovnání s celkovým počtem obcí v ČR bylo osloveno v průměru 82,75% všech obcí.

Graf č.2 Počet oslovených obcí v jednotlivých krajích ČR vs. počet obcí v krajích

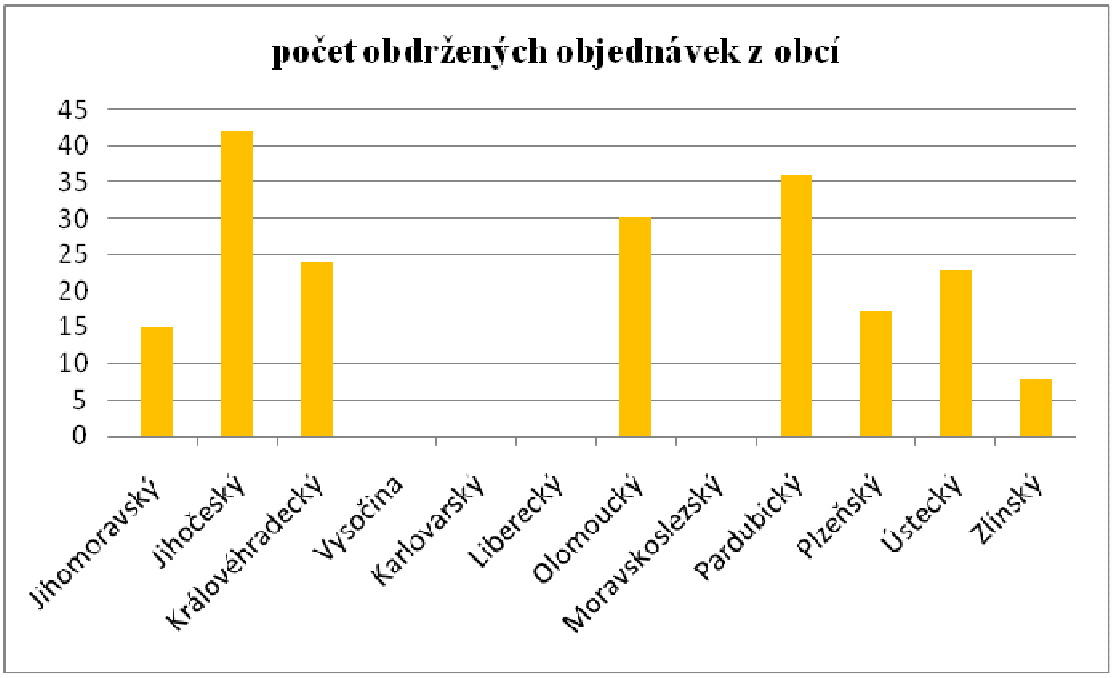


Zpětná vazba na odeslané nabídky činila v průměru 26,56%. Z tohoto podílu byla následující odpověď:

- již jsme školení absolvovali 42%
- školení máme objednané a budeme absolvovat 32%
- necítíme potřebu školení absolvovat 15%
- jiná odpověď 8%

Efekt návratnosti emailu a následného objednání služby se rovnal průměru marketingových aktivit v této oblasti. A nijak nevybočoval z obvyklých standardů. Činil 3,67% z obeslaných obcí a 3,53% ze všech obcí v České republice.

Graf č.3 Počet obdržených objednávek z obcí v ČR



Dalším důležitým krokem byla komunikace s jednotlivými obcemi ohledně sledění termínů a počtu účastníků. 2 externě najatí a proškolení lektoři provedli v dohodnutých termínech školení, které se ve 100% případů podařilo realizovat v místě objednatele. Čímž odpadávaly pro objednavatele další náklady spojené s výjezdem zaměstnanců. Jako například cestovné, vyplácení diet atd..

Každý z krajských úřadů v ČR měl ve svém rozpočtu zahrnutu položku: „Školení datových schránek pro obce“ (či rozpočtovou položku podobného znění) Při minianketě uskutečněné v rámci realizace vyšla najevo závažná skutečnost, že 99% z obcí, které se školení účastnilo, neobdrželo informaci o tom, že je možné se nechat proškolit zdarma v rámci spolupráce s Krajským úřadem. Respektive, že Krajský úřad je připraven zajistit technicky i finančně oblast školení kolem spuštění provozu datových schránek.

Výše uvedený graf je reálnou skutečností. Poskytuje tedy informaci o tom, jakým způsobem ten který Krajský úřad komunikuje jako nadřízený orgán s obcemi v regionu. A především signalizuje určité nekomfortnosti v oblasti zavádění datových schránek do státní správy. Pokud je schopna privátní firma uspět na trhu s nabídkou služby, kterou má nadřízený orgán obce, nebo by měl, zajišťovat zdarma v rámci svých činností, je otázkou jak kvalitně byla tato činnost ze strany státu, potažmo krajského úřadu provedena. A to především v oblasti „interního“ marketingu. S ohledem na hierarchii státní správy a samosprávy a termín, který přímo navazoval na oficiální spuštění provozu datových schránek, by se dalo očekávat, že ve výše uvedeném období již bude minimálně převážná většina obcí v práci s datovými schránkami proškolena.

6. VÝHODY A NEVÝHODY VYUŽITÍ DATOVÝCH SCHRÁNEK VE STÁTNÍ SPRÁVĚ

1. Zrychlení a zefektivnění komunikace

Nesporným faktem je, že elektronická komunikace sama o sobě je komfortnějším a rychlejším způsobem výměny informací. Zaměstnanci veřejné správy „vázaní“ na papírovou dokumentaci jsou právě tou cílovou skupinou, pro kterou bude splnění bodů z pohledu zrychlení a zefektivnění komunikace pravděpodobně největším problémem.

2. Zřízení konsolidované datové základny, využitelná pro konstrukci informačního obsahu a aplikací.

Zvýšené náklady orgánů veřejné moci v první fázi spojené s nezbytnými úpravami některých stávajících informačních systémů již pravděpodobně nebude nikdo schopen vyčíslit. Vyčíslení by bylo zajímavé z pohledu efektivity implementace a provozu datových schránek. Konkrétně by bylo vhodné vyčíslit minimálně náklady s úpravami rozhraní pro zajištění komunikace s informačním systémem datových schránek, s přizpůsobením systému spisové služby, s vybavením pro provádění autorizované konverze. Kteroukoliv vládou proklamované snižování nákladů ve státní správě dostává v tomto případě trhlinu v podobě nemožnosti vyčíslit náklady a tím pádem i úspory a to jak z hlediska personálního, tak i z hlediska přínosu pro občana.

3. Ucelený balík zákonů jako právní základ a opora e-Governmentu

Vytvořený soubor zákonů je jeden z nejdůležitějších bodů, který ČR alespoň částečně posouvá mezi země, které kladou velký důraz na využití informačních technologií ve veřejné správě a zároveň pro tuto činnost vytváří legislativní oporu.

„ Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, ve znění pozdějších předpisů upravuje elektronické úkony, a to mezi fyzickými a právnickými osobami a orgány veřejné moci oběma směry, případně mezi

orgány veřejné moci navzájem. Otázkou je, zda se tím myslí pouze právní úkony, či nikoliv.“ (Datové schránky v právním řádu ČR, prof. Ing. Vladimír Smejkal, CSc. LL.M. 2009, str.30)

prof. Ing. Vladimír Smejkal, CSc. LL.M. dále uvádí, že „ Je tedy nutno chápat formulaci „elektronické úkony“ v širším slova smyslu, tj. jako jakoukoliv činnost orgánu veřejné moci, kde tento orgán vystupuje z pozice úřadu vykonávajícího veřejnou moc, nikoliv kdy sám vstupuje do soukromoprávních vztahů – např. s dodavateli.“ (Datové schránky v právním řádu ČR, 2009, str.30)

4. **Robustní, bezpečná a efektivní infrastruktura, schopná zprostředkovat přístup k datovým zdrojům s potenciálem dalšího rozvoje.**

Informační systém datových schránek by měl být koncipován takovým způsobem, aby mohl být postupně rozšiřován pro použití s dalšími formáty datových zpráv. To umožní postupné převádění agendy zajišťované jinými informačními systémy veřejné správy do informačního systému datových schránek. Pokud jde o návaznost na elektronickou spisovou službu, záleží na rozhodnutí jednotlivých orgánů veřejné moci, zda doručenou datovou zprávu budou dále zpracovávat v elektronické podobě, nebo uplatní smíšený model. Což je možno považovat za problematické s ohledem na financování celého procesu. V období, kdy mohla veřejná správa čerpat dotační tituly na informační systémy, včetně implementace HW a SW na datové schránky, mělo být direktivně určeno, respektive měla být stanovena kritéria, kdo je povinen zpracovávat datové zprávy v elektronické podobě a kdo ne. Tedy jasně stanoveno, kdo, za jakých podmínek a jak musí doručenou datovou zprávu dále zpracovávat. Připravovaná novela zákona o archivnictví a spisové službě, která vymezí vedení spisové služby a způsoby práce s elektronickými dokumenty, bude s největší pravděpodobností určovat i kritéria toho, jakým způsobem jsou organizace povinny doručenou zprávu dále zpracovávat. V případě použití systému spisové služby bude pro velkou část uživatelů nemalým problémem zajištění financování.

5. **Sada klíčových aplikací usnadňující řešení běžných životních situací, podnikání a komunikaci se státní administrativou (s přesahem do komerční sféry)**

   Z důvodu technických omezení systému datových schránek nelze zasílat zprávu o větším objemu než 10 MB. Není pravděpodobně na denním pořádku odesílání takto objemných zpráv, nicméně technická omezení tohoto druhu mohou v některých případech velice komplikovat běžný provoz.

6. **Snížení administrativních nákladů spojených s chodem veřejné správy v souvislosti se zaváděním e-Governmentu o 20 % do roku 2013 oproti stavu před spuštěním e-Governmentu)**

   Tento bod úzce souvisí s tezemi v bodě 1 této kapitoly.
   Jakým způsobem bude tato úspora dokladována a vyčíslena, na to si budeme muset počkat. Jednoznačné je to, že ekonomický přínos a efekt bude tím nejzákladnějším kritériem hodnocení. Osobně bych očekával vyčíslení výše zmiňovaných úspor jak na straně finanční, tak i na straně personální. Potom se dá kvalifikovaně hovořit efektivní implementaci a zavedení systému datových schránek spolu s pokračujícím trendem eGovernmentu.
   Pro příklad situace a pozice České pošty v systému eGovernmentu, ze které je patrné, , že Česká pošta je i nadále společnost vlastněná státem.
   Česká pošta přichází kvůli elektronické komunikaci s úřady o peníze za doporučené dopisy. Konkrétně je uváděno 1,5 miliardy korun za rok. Za provoz datových schránek si přitom vydělá odhadem zhruba 800 milionů korun. Rozdíl 700 miliónů korun chce Česká pošta pokrývat například takzvaným bezpečným klíčem k datové schránce. Což je dle informací České pošty prostředek bezpečného přihlášení, bezpečnějšího přihlášení k datové schránce, založený na komerčním certifikátu. Současný způsob přihlašování je tedy ne dostatečně bezpečným? Pro datové schránky nabízí Česká pošta také takzvaný datový trezor, tedy úložiště elektronických dokumentů. Cenově naprosto nezajímavá nabídka České pošty (uložení: do 100 zpráv 1.200,-Kč bez DPH/rok, do 500 zpráv 5.400,-Kč bez DPH/rok a do 5000 zpráv 48.000,-Kč bez DPH/rok), kdy tedy uložení 1 zprávy stojí ročně v rozmezí 9,6 – 12 Kč bez DPH bude

asi těžko konkurovat datovým uložištím komerční sféry. Další součástí těchto komerčních služeb je například notifikace, tedy upozornění na příchozí datovou zprávu pomocí SMS zprávy. Celkovým dojmem je tedy přenášení nákladů státní správy na podnikatelskou sféru a to způsobem, který je v rozporu s proklamovaným heslem „Obíhat mají dokumenty a ne občané“, ale za čí peníze?

7. Bezpečnost komunikace

Dalším problémem, který se objevil, bylo, je a stále trvá útočení hackerů na přihlašovací údaje. Je jasné, že systémem se zasílají velmi citlivé údaje, mnohdy přímo spojené s informacemi o finančních otázkách, a proto se nelze divit různým amatérským či profesionálním útokům ze strany hackerů na celý systém. Provozovatel systému Česká pošta nebyla na tento problém dokonale připravena a musela implementovat řadu bezpečnostních řešení za ostrého běhu systému po datu 1. listopadu 2009. Útoky na datové schránky nevykazovaly a ani nevykazují vysoce sofistikované řešení, tak jako například útoky na bankovní účty. Výsledek takového útoku lze jen těžko zpeněžit. Hlavním způsobem bývá falešná adresa typu www.datoveschranky.** a hlavním důvodem bývá sběr dat a jejich zneužití v konkurenčním boji v tržním prostředí.

8. Úspora nákladů (poštovné, kancelářský materiál)

Jak bylo uvedeno v bodě 5 této kapitoly, prokazování úspor v oblasti zprovoznění a provozu datových schránek, pokud nebyl systém nastaven již na počátku, bude velice problematické.

Česká pošta je oficiálním provozovatelem datových schránek. Funkce jí připadla ze zákona jako náhrada za ztrátu způsobenou úbytkem klasické korespondence. Ročně za to bude od státu inkasovat odhadem kolem 200 milionů korun. Telefónica O2 implementovala datové schránky, inkasuje část výdělku z každé zprávy odeslané uvnitř systému. Firma Software602 je autorem "ovladače", bez nějž není možné se dostat přes základní rozhraní k obsahu datové zprávy. Software602 je subdodavatelem

Telefóniky O2. Další IT firmy vydělávají na přechodu státní správy i firem na komunikaci přes datové schránky. Pro větší instituce připravují vnitřní systémy distribuce datových zpráv – takzvané spisové služby – nebo upravují jejich stávající. Cena zavedení spisové služby se pohybuje v řádu statisíců až milionů korun.

9. Přístupnost z kteréhokoliv místa planety (přes internet)

Až po mnohých urgencích z řad uživatelů byla v říjnu 2010 provedena aktualizace informačního systému datových schránek. Náhled datové zprávy umožní zobrazit obsah datové zprávy a stáhnout vložené přílohy, a to i v případě, že na počítači není nainstalovaný doplněk 602XML Filler, který je vyžadován v případě, že je používán k práci s datovou schránkou webový portál. Bez doplňku nejsou k dispozici některé důležité informace týkající se zabezpečení datové zprávy (časové razítko a elektronická-značka).

Tento přístup je určen těm, kteří se rychle potřebují seznámit s datovou zprávou – například na dovolené, a nemají přitom k dispozici svůj počítač. V tomto režimu není možné datové zprávy vytvářet, lze se jen seznámit s obsahem došlé zprávy a je možné si stáhnout a vytisknout i všechny její přílohy. Lze tedy hovořit o přístupnosti z kteréhokoliv místa planety, ale je také nutné hovořit o přístupu omezeném.

10. Úspora času

Jeden z bodů, který splňuje požadavky moderní státní správy. Čas strávený na poště vyzvedáváním doporučených dopisů atd. je opravdu k nezaplacení.

11. občanům je tato služba poskytována zdarma

Ano ze strany státní správy je to pravdou. Pokud pomineme náklady z bodu 5 a 7 této kapitoly, které ve svém důsledku nese stejně tak jako tak daňový poplatník.

Nevýhody a problémy digitalizace dokumentů

Mimo jiné výše uvedené nevýhody a problémy implementace a provozu datových schránek lze zařadit také:

1. chybné, nebo nejasné chápání pojmu listina, písemnost, dokument apod.
2. přílohy, které nelze v elektronické podobě doručovat
3. negativní přístup k zákonu o archivnictví a spisové službě
4. touha mít v ruce papír

7. DATOVÉ SCHRÁNKY A JEJICH VYUŽITÍ U PRÁVNICKÝCH OSOB (V KOMERČNÍ SFÉŘE)

I když zákon o elektronických úkonech a autorizované konverzi dokumentů začal platit od 1. července 2009, povinnost schránku používat byla odsunuta na první listopad 2009. Od tohoto data byla komunikace prostřednictvím datových schránek pro právnické osoby a orgány veřejné moci povinná. Živnostníci podnikající jako fyzické osoby a ostatní občané si je mohou založit podle vlastního uvážení.

Ministerstvo vnitra nejdříve nabídlo budoucím uživatelům datových schránek možnost bezplatného vyzkoušení jejich provozu. Testovací verze elektronické datové schránky byla prakticky shodná se skutečnou datovou schránkou, kterou si budoucí uživatel povinně nebo dobrovolně od července 2009 aktivoval.

Fyzická osoba, podnikající fyzická osoba nebo právnická osoba může provádět podání vůči orgánu veřejné moci prostřednictvím své datové schránky, má-li zpřístupněnou datovou schránku a povaha podání to umožňuje. Podání prostřednictvím datové schránky má stejný dopad jako podepsané písemné podání. Odesílatel obdrží zprávu o dodání podání do datové schránky nebo mu je sdělena informace o neúspěchu dodání (např. že datová schránka adresáta byla zrušena nebo není zpřístupněna). Zpráva bude opatřena uznávanou elektronickou značkou ministerstva.

Datovou schránku zřizuje Ministerstvo vnitra ČR zájemcům bezplatně, do tří pracovních dnů ode dne podání žádosti. Následně jim pošta do vlastních rukou doručí přístupové údaje k datové schránce. Do datové schránky bude mít přístup pouze její zřizovatel a osoba, kterou tím pověří. Heslo určené k otevření schránky není totožné s přiděleným identifikátorem schránky. Pro subjekty, které o to požádají, by měl být k dispozici přístup s vyšší mírou zabezpečení. Občané a podnikatelé mohou informační systém datových schránek bez dalších nákladů používat prostřednictvím webového prohlížeče.

8. VÝHODY A NEVÝHODY VYUŽITÍ DATOVÝCH SCHRÁNEK U PRÁVNICKÝCH OSOB (V KOMERČNÍ SFÉŘE)

Výhody datových schránek:

- Jednoduché a snadno pochopitelné ovládání
- Podobnost s emailovou poštou

Nevýhody datových schránek:

- Nutnost ukládat doručené zprávy mimo datovou schránku
- U počítačů s pomalejším připojením zdlouhavé otevírání doručených nebo odeslaných zpráv

V roce 2010 prošla systémem dle informací České pošty 10 miliontá zpráva. I přes to se ozývají hlasy odborníků o tom, že systém má stále řadu rezerv. Například z pohledu zákonné úpravy, která není dodnes jednoznačná, a s ohledem na tuto skutečnost se na potřebných náležitostech celá řada institucí neshoduje. Část uživatelů z řad podnikatelů i úřadů činí při přebírání a zasílání datových zpráv fatální chyby, které mohou znamenat v konečném důsledku milionové ztráty na všech stranách.

Stav kolem zaručenosti a časové pomíjivosti elektronického podpisu, který se projevuje již od doby spuštění systému, není také zanedbatelným problémem. Jediným dostatečně spolehlivým a bezpečným způsobem je, že si pro kořenové certifikáty CA PostSignum zajdeme přímo na pracoviště samotné certifikační autority PostSignum – protože zde můžeme předpokládat, že nám dají (nakopírují na naše USB či CD apod.) skutečně své certifikáty. Podobně bychom mohli zajít na nějakou provozovnu České pošty. Vhodným způsobem by například bylo i to, pokud by Česká pošta distribuovala kořenové certifikáty svých CA spolu s přihlašovacími údaji k datovým schránkám na nosiči vloženém do obálky. Bohužel touto variantou se nikdo nezabýval. Poté již máme k dispozici ne 100% spolehlivé varianty, které by se za určitých okolností bylo možno využívat, ale je nutno konstatovat, že v nabídce České pošty nejsou taktéž. Například: Příslušné certifikáty by bylo možno stáhnout z webu, z nějakého dosud neověřeného zdroje. To vše za podmínky, že následně dojde k dostatečně spolehlivému ověření jejich pravosti. Tím je porovnání hashe certifikátů, stažených z webu, s hodnotou získanou z dostatečně spolehlivého zdroje. Spolehlivým zdrojem by opět mohla

být zásilka České pošty s kódem. Zásadním problém celé situace se tedy jeví skutečnost, že nikdy nemáme zaručeno, zda hash stahujeme ze skutečných stránek PostSignum či MV ČR a nebo z nějakých nelegálních stránek. Neexistuje tedy bezpečnější resp. bezpečná varianta než ta, že si pro kořenové certifikáty CA PostSignum zajdeme přímo na pracoviště samotné certifikační autority PostSignum nebo na pracoviště CzechPoint.

Obzvláště začínající podnikatelé se potýkají s problémem při registraci na finančním úřadě, respektive po této registraci. Finanční úřad požaduje potvrzení o registraci aktivace datové schránky, ale skutečnost je taková, že doručovací informace jsou zasílány až později. Pokud tedy finanční úřad zasílá nově vzniklému podnikateli zprávu, tak ji zasílá do nefunkční datové schránky.

Od spuštění ostrého provozu datových schránek jsou medializovány případy z oblasti exekučního řízení, které mohou do budoucnosti způsobovat právní nejistotu. Jeden z možných nedostatků náležitostí datových zpráv – chybějící elektronický podpis – může způsobit, že rozhodnutí se stane nevykonatelným. Podnikatelé a firmy se potom budou muset bránit platbám za škody, které mohou dosáhnout až řádů milionů korun. Rozhodnutí zaslané bez elektronického podpisu má jen informativní charakter a není možné ho právně uznat. Pro příjemce neznamená žádná práva ani povinnosti. Může se ovšem domáhat doručení validního rozhodnutí. A pokud, hypoteticky vzato, vznikne podnikateli z tohoto stavu škoda, je oprávněn žádat její náhradu. Důvodem je nesprávný úřední postup.

Zřizování datových schránek pro podnikatele více méně prokázalo tristní stav informací, které o nás a o podnikatelích stát uchovává. Po zaslání žádosti následovala procedura schvalování na ministerstvu vnitra. Pokud bylo vše v pořádku a informační systém evidence obyvatel nenašel nesrovnalosti, tak z velké části automaticky přidělil údaje, ale na závěr musel stejně vše zkontrolovat a schválit úředník. V opačném případě, kdy byly nalezeny rozdíly mezi žádostí a daty v informačním systému evidence obyvatel, se celý proces děl manuálně. Úředník kontroloval údaje na straně informačního systému údaje a hledal chyby. To byl častý důvod zpožděného dodání údajů nutných ke spuštění datové schránky žadatelům. Bohužel nikdo tyto žadatele neinformoval o tom, že celý proces je z těchto důvodů ve zpoždění. Je ovšem nutno konstatovat, že velká část podnikatelů nechala celou proceduru úplně na

poslední a nejzazší termín, tak jak bývá v našich krajích zvykem. Například při odevzdávání daňových přiznání, výměně občanských či řidičských průkazů apod…

Zavedení datových schránek má jedno velké pozitivum. Někteří podnikatelé, kteří zatím dokázali i několik let hrát úspěšně se státem hru na schovávanou, se dostávají do problému. V České republice existují určitě tisíce firem, na které nezůstaly ostatním podnikatelům zrovna růžové vzpomínky. Ti se mohou konečně domoci výkonu práva, protože před zřízením datových schránek nebylo možné druhé straně doručit předvolání, obsílku atd. Datová schránka resp. zákon praví v přeneseném slova smyslu: sem bude stát podobné dokumenty dodávat a pokud nebudou vyzvednuty do určité lhůty, *považují se za doručené*, takže může zasednout např. soud, vynést rozsudek atd.

9. KVALITA ŘEŠENÍ, PROPAGACE, STAV VYUŽITÍ V ROCE 2010, ČESKÁ POŠTA, MINISTERSTVO VNITRA

Novela zákona k datovým schránkám označovaná jako verze 2.0 přinesla několik významných změn. Jedna z nich se týká způsobu financování. Ve stávající právní úpravě zákona č. 300/2008 Sb. je tato otázka financování řešena ne dost konkrétně prostřednictvím § 14 jako o odměně provozovatele informačního systému. Odměna držiteli poštovní licence za provozování informačního systému datových schránek se stanoví podle cenových předpisů, následuje odkaz na zákon o cenách. Ale kdo bude platit? Zřizovatel a správce datových schránek, kterým je Ministerstvo vnitra? Nebo budou platit jednotliví uživatelé datových schránek? Tedy všechny orgány veřejné moci, a také právnické osoby zapsané v obchodním rejstříku, tedy všichni, kteří si nechají schránku zřídit dobrovolně?

V únoru 2009, došlo k částečnému narovnání situace, kdy Ministerstvo vnitra podepsalo s Českou poštou smlouvu o provozování informačního systému datových schránek, a byly domluveny i cenové podmínky.

Tabulka č.1 Ceník České pošty

Hranice	**Cena služby pro uživatele**	**Cena služby pro uživatele**
Transakcí kumulativně	**Cena s DPH**	Cena bez DPH
0-33 mil	**17,90**	15,04
33 - 66 mil	**15,90**	13,36
66 - 100 mil.	**13,90**	11,68
100 - 123 mil.	**11,90**	10,00
nad 123 mil.	**9,90**	8,32

Díky zpoplatnění datových schránek lze uvažovat i o významném rozšíření jejich využitelnosti. Jejich původní náplň totiž byla zajistit přenos zpráv „od“ nebo „k“ orgánům veřejné moci, včetně přenosu mezi orgány veřejné moci. Dá se říci: alespoň na jedné straně přenosu musel vždy být orgán veřejné moci.

Pokud použijeme obvyklé „úřední“ terminologie to lze charakterizovat jako:

- **doručování**, kdy zprávu odesílá orgán veřejné moci a jejím příjemce je subjekt, vybavený datovou schránkou (ať již jde o orgán veřejné moci, právnickou či fyzickou osobu). Zde je použití datové schránky povinné.
- **podávání**, kdy zprávu odesílání právnická či fyzická osoba (resp. jiný subjekt než orgán veřejné moci), a příjemcem je naopak orgán veřejné moci. Zákon 300/2008 Sb. toto definuje jako „provádění úkonů vůči orgánům veřejné moci“, v praxi jde o různá podání vůči nim. Využití datových schránek je zde volitelné, nikoli povinné.

Výše uvedená novela rozšiřuje možnosti využití datových schránek, a to o přenos zpráv obecně mezi všemi subjekty, které datové schránky mají. Hospodářská komora prosadila do novely pozměňovací návrhy, které takovéto využití umožňuje.

Zavádí se tím další varianta přenosu prostřednictví, datové schránky, která je označována jako:

- dodávání, vymezené jako přenos dokumentů mezi datovými schránkami fyzických nepodnikajících osob, fyzických podnikajících osob a právnických osob.

S „dodáváním“ je navíc spojena i sankce pro případ zneužití datových schránek ke spammingu. Spamming je zde vymezen šíře, než ve smyslu stávajícího zákona o některých službách informační společnosti (zákona č. 480/2004 Sb.): nikoli jen jako nevyžádané obchodní sdělení, ale i jako „jiné obtěžující sdělení“. A dokonce jsou stanoveny i sankce: pro nepodnikající fyzické osoby až 10 000 Kč, a pro ostatní (podnikající) až 10 000 000 Kč.

Je zde i pamatováno na zneužití datových schránek k šíření „počítačového programu, který může poškodit informační systém datových schránek, údaj v něm obsažený nebo výpočetní techniku držitele datové schránky“. V těchto případech je zneužití sankcionováno 2x vyšší sazbou než u spammingu. A to i přes to, že před spuštěním ostrého provozu se všichni zainteresovaní hlásili k tezi, že přenos jakéhokoli škodlivého kódu skrze datové schránky nebude možný. V rozporu s výše uvedenou skutečností je otázka resp. odpověď uveřejněná na www.datoveschránky.info [2011-03-21]v sekci 04 (časté dotazy v části technické požadavky):

Bude informační systém kontrolovat, zda datová zpráva není nebezpečná pro systém, pokud ano, je informační systém oprávněn zprávu odstranit? Je taková zpráva považována za doručenou? Bude o odstranění informován i adresát?

ISDS zprávu obsahující škodlivý kód odmítne přímo na vstupu, tzn. zpráva není vůbec přijata a tudíž nemůže být doručena. Adresát o tom nebude informován. Dostupné: http://www.datoveschranky.info/technicke-pozadavky/ [2011-03-21]

Sankcionovány mohou být fyzické i právnické osoby ne tak orgány veřejné moci. Asi se předpokládá, že by se ve státní správě někdo něčeho takového mohl dopustit. Co například notáři, nebo exekutoři? Ti jsou také orgány veřejné moci.

10. ZÁVĚR

O budoucnosti datových schránek se v současné době moc nehovoří. I na serveru www.egonacademy.cz, kde by měla být jedna část věnována dle titulku“ Budoucnost komunikace občana se státem“ budoucnosti, lze spustit jen video, na kterém se hovoří pouze o základních registrech, záměny rodného čísla za jiný identifikační ekvivalent a o občanském průkazu jako dokladu pro veškerý styk se státní správou.

Připravovanou motivací pro zřízení datové schránky občany může být například doručování výpisů trestných bodů z karty řidiče. Nebo tak zvaný. e-voting (e-volby) tj. způsob voleb, kdy občané voliči volí prostřednictvím počítače a internetu. Mimo jiné technické a administrativní problémy by bylo nutné zamezit riziku voleb pod nátlakem resp. kupování hlasů. Po komunálních volbách v roce 2010, kdy bylo v některých obcích nutno volby opakovat z důvodů kupování hlasů několikrát, lze tento bod považovat za nejkritičtější. Navíc Ústava České republiky požaduje volby tajné, všeobecné, rovné a přímé. A hlasování prostřednictvím počítače je s ohledem na přímost volby diskutabilní.

Abych nezdůrazňoval pouze nevýhody, či kontroverzní přínos systému datových schránek, pozitivně je nutno ocenit fakt, že datové schránky nastoupily na sice obtížnou, ale správnou a perspektivní cestu elektronického doručování. Zároveň došlo k vytvoření sítě takzvaných Czech POINTů, díky kterým mohou osoby soukromého práva komunikovat s úřady a státními institucemi.

Pro posouzení celkové bilance (zda datové schránky přinesou celkové úspory, nebo naopak vyšší náklady) je ale třeba vzít v úvahu i další faktory, a ne pouze samotné ceny za přenos zpráv skrze datové schránky. Co další náklady, které si zavedení datových schránek vynutí? Od jednorázových upgradů spisových služeb, přes zaškolení uživatelů, až po průběžné náklady na konverze všude tam, kde nebude možné či účelné dále pracovat s elektronickou verzi dokumentu, dodanou skrze datovou schránku.

11. POUŽITÁ LITERATURA

Vít Lidinský a kol., *eGovenrment bezpečně,* Grada Publishing a.s. 2008, 145stran, ISBN 978 – 80 – 247 – 2462 – 1

Prof. Ing. Vladimír Smejkal, **CSc. LL.M.**, Datové schránky v právním řádu ČR, ABF a.s. 2009, 176 stran, ISBN 978 – 80 – 86284 – 78 – 1

JUDr. Bohumír Štědroň, **LL.M.**, Úvod do eGovernmentu, Úřad vlády České republiky 2007, 176 stran, ISBN 978 – 80 – 87041 – 25 – 3

Internetové zdroje

eGovernment, From Wikipedia, the free encyclopedia.

Dostupný na WWW : http://en.wikipedia.org/wiki/EGovernment [cit. 2011-03-21]

Portál Ministerstva vnitra ČR

Dostupný z WWW: http://www.mvcr.cz/ [cit. 2011-03-21]

Magazín eGovernment – 2010

Dostupný z WWW: http://www.egovernment.cz/default.htm [cit. 2011-03-21]

ISVS.CZ - Informační Systémy Veřejné Správy

Dostupný z WWW: http://www.isvs.cz/ [cit. 2011-03-21]

Portál veřejné správy

Dostupný z WWW: www.portal.gov.cz [cit. 2011-03-21]

Czech POINT

Dostupný z WWW: http://www.czechpoint.cz/web/index.php [cit. 2011-03-21]

UNCITRAL

Dostupný z WWW: http://www.uncitral.org/uncitral/en/index.html [cit. 2011-03-21]