Datové schránky a jejich fungování ve veřejné správě

Petr Heinisch

Bakalářská práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky

Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky
Ústav regionálního rozvoje, veřejné správy a práva
akademický rok: 2011/2012

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Petr HEINISCH**
Osobní číslo:	**M09216**
Studijní program:	**B 6202 Hospodářská politika a správa**
Studijní obor:	**Veřejná správa a regionální rozvoj**
Téma práce:	**Datové schránky a jejich fungování ve veřejné správě**

Zásady pro vypracování:

Úvod

I. Teoretická část

- **Popište systém elektronické veřejné správy.**
- **Popište informační systém datových schránek.**
- **Popište proces implementace datových schránek v české elektronické veřejné správě.**

II. Praktická část

- **Analyzujte využití datových schránek v České republice orgány veřejné moci, právnickými osobami a ostatními.**
- **Analyzujte problémy spojené s požíváním datových schránek.**
- **Navrhněte řešení problémů spojených s požíváním datových schránek.**

Závěr

Rozsah bakalářské práce: **cca 40**

Rozsah příloh:

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

Seznam odborné literatury:

[1] BUDIŠ, P. a HŘEBÍKOVÁ, I. Datové schránky: fungování, doručování, bezpečnost, návody. 1. vyd. Olomouc: ANAG, 2010. 287 s. ISBN 978-80-7263-617-4.
[2] MATES, P. a SMEJKAL, V. E-government v českém právu. Praha: Linde, 2006. 244 s. ISBN 80-7201-614-8.
[3] ŠTĚDROŇ, B. Úvod do eGovernmentu v České republice: právní a technický průvodce. 1. vyd. Praha: Úřad vlády České republiky, 2007. 172 s. ISBN 978-80-87041-25-3.

Vedoucí bakalářské práce: **Mgr. Tomáš Pavlíček**
Ústav regionálního rozvoje, veřejné správy a práva

Datum zadání bakalářské práce: **2. dubna 2012**

Termín odevzdání bakalářské práce: **18. května 2012**

Ve Zlíně dne 2. dubna 2012

prof. Dr. Ing. Drahomíra Pavelková
děkanka

L.S.

RNDr. Oldřich Hájek, Ph.D.
ředitel ústavu

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ/DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- odevzdáním bakalářské/diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby[1];

- bakalářská/diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému,

- na mou bakalářskou/diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3[2];

- podle § 60[3] odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;

---

[1] *zákon č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, § 47b Zveřejňování závěrečných prací:*

(1) Vysoká škola nevýdělečně zveřejňuje disertační, diplomové, bakalářské a rigorózní práce, u kterých proběhla obhajoba, včetně posudků oponentů a výsledku obhajoby prostřednictvím databáze kvalifikačních prací, kterou spravuje. Způsob zveřejnění stanoví vnitřní předpis vysoké školy.

(2) Disertační, diplomové, bakalářské a rigorózní práce odevzdané uchazečem k obhajobě musí být též nejméně pět pracovních dnů před konáním obhajoby zveřejněny k nahlížení veřejnosti v místě určeném vnitřním předpisem vysoké školy nebo není-li tak určeno, v místě pracoviště vysoké školy, kde se má konat obhajoba práce. Každý si může ze zveřejněné práce pořizovat na své náklady výpisy, opisy nebo rozmnoženiny.

(3) Platí, že odevzdáním práce autor souhlasí se zveřejněním své práce podle tohoto zákona, bez ohledu na výsledek obhajoby.

[2] *zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 35 odst. 3:*

(3) Do práva autorského také nezasahuje škola nebo školské či vzdělávací zařízení, užije-li nikoli za účelem přímého nebo nepřímého hospodářského nebo obchodního prospěchu k výuce nebo k vlastní potřebě dílo vytvořené žákem nebo studentem ke splnění školních nebo studijních povinností vyplývajících z jeho právního vztahu ke škole nebo školskému či vzdělávacího zařízení (školní dílo).

[3] *zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 60 Školní dílo:*

(1) Škola nebo školské či vzdělávací zařízení mají za obvyklých podmínek právo na uzavření licenční smlouvy o užití školního díla (§ 35 odst. 3). Odpírá-li autor takového díla udělit svolení bez vážného důvodu, mohou se tyto osoby domáhat nahrazení chybějícího projevu jeho vůle u soudu. Ustanovení § 35 odst. 3 zůstává nedotčeno.

- podle § 60[4] odst. 2 a 3 mohu užít své dílo – bakalářskou/diplomovou práci - nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);

- pokud bylo k vypracování bakalářské/diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské/diplomové práce využít ke komerčním účelům.

Prohlašuji, že:

- jsem bakalářskou/diplomovou práci zpracoval/a samostatně a použité informační zdroje jsem citoval/a;

- odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně 10.5.2012 Petr Heinisch

[4] *zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 60 Školní dílo:*

(2) Není-li sjednáno jinak, může autor školního díla své dílo užít či poskytnout jinému licenci, není-li to v rozporu s oprávněnými zájmy školy nebo školského či vzdělávacího zařízení.

(3) Škola nebo školské či vzdělávací zařízení jsou oprávněny požadovat, aby jim autor školního díla z výdělku jím dosaženého v souvislosti s užitím díla či poskytnutím licence podle odstavce 2 přiměřeně přispěl na úhradu nákladů, které na vytvoření díla vynaložily, a to podle okolností až do jejich skutečné výše; přitom se přihlédne k výši výdělku dosaženého školou nebo školským či vzdělávacím zařízením z užití školního díla podle odstavce 1.

ABSTRAKT

Tato bakalářská práce se v teoretické části zabývá elektronickou veřejnou správou, a to jejím legislativním vymezením, vývojem a stručným popisem eGovernmentu v rámci EU a systémem eGovernmentu v České republice, informačním systémem datových schránek, kde jsou vymezeny pojmy z této oblasti a také procesy, s nimiž se uživatelé datových schránek mohou setkat, a v poslední části je popsán proces zavádění datových schránek v České republice. Praktická část se zaměřuje na využití datových schránek jednotlivými subjekty, popis problémů, s nimiž je možno se při využívání datových schránek setkat, a následně návrhy řešení těchto problémů.

Klíčová slova:

eGovernment, informační systémy veřejné správy, informační systém datových schránek, datová schránka, autorizovaná konverze dokumentů, elektronický podpis, Czech POINT, zákon o elektronických úkonech a autorizované konverzi dokumentů

ABSTRACT

This Bachelor Thesis deals in its theoretical part with eGovernment, its legislative definition, evolution and a brief description of eGovernment within the EU, and the system of eGovernment in the Czech Republic, with data boxes information system where there are defined terms from this field as well as processes which data boxes users may encounter, and in the last section, the process of data boxes implementing in the Czech Republic is described. The practical part is focused on the use of data boxes by individual entities, on description of problems possible to encounter while using data boxes, and subsequently on proposals of solving these problems.

Keywords:

eGovernment, public administration information systems, data boxes information system, data box, authorized conversion of documents, electronic signature, Czech POINT, electronic transactions and authorized conversion of documents law

Děkuji Mgr. Tomáši Pavlíčkovi za vedení mojí bakalářské práce a za připomínky a náměty, které mi poskytnul v průběhu jejího vypracování.

Také děkuji všem, kdo mi jakkoli pomáhali.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Stejně jako v podstatě každá oblast lidské činnosti i výkon veřejné správy a komunikace občanů, podnikatelů a jiných subjektů s ní prochází přirozeným vývojem, který je spojen především se stále významnějším využitím moderních informačních a komunikačních technologií. I když klasická komunikace formou papírových dokumentů s razítky a podpisy je stále užívaná, je přechod na elektronickou formu výkonu veřejné správy stále patrnější a dochází k jeho neustálému rozšiřování, a to nejen vzájemně mezi úřady, ale i mezi úřady a ostatními subjekty.

Z tohoto důvodu bylo nutné vytvořit prostředek, jenž bude efektivně sloužit při elektronizaci veřejné správy, tedy datových schránek. Jejich zavedení v České republice v druhé polovině roku 2009 přineslo orgánům veřejné správy a některým dalším orgánům povinnost využívat je jako jediný prostředek ke komunikaci, a alespoň u těchto subjektů je tak dnes papírová komunikace zcela nahrazena elektronickou formou. Tuto situaci lze označit za nejrazantnější změnu v oblasti státní správy v historii České republiky.

Mým záměrem je touto prací datové schránky přiblížit zejména běžnému občanovi, pro kterého je sice zřízení datové schránky nepovinné, avšak vlastnit ji přináší v mnoha ohledech pohodlnější komunikaci s úřady, především z hlediska úspory času potřebného k vyřízení určité záležitosti. Na druhé straně je logické, že ani informační systém datových schránek se nepodařilo zavést, aniž by se vyskytly určité problémy, a proto se i jim a jejich předcházení a řešení tato práce věnuje.

I. TEORETICKÁ ČÁST

1 SYSTÉM ELEKTRONICKÉ VEŘEJNÉ SPRÁVY

1.1 eGovernment – vymezení pojmu

Slovo „eGovernment“ vzniklo spojením anglických slov „electronic“ a „government“, tedy doslovně „elektronické vládnutí“. Jedná se o elektronizaci veřejné správy a samosprávy, o přechod vedení agendy na elektronickou verzi. K úpravě vztahů dochází jak na vnitřní tak i na vnější úrovni veřejné správy, a to pomocí nových informačních technologií.

Za hlavní záměr eGovernmentu lze označit zejména zefektivnění komunikace veřejnosti s úřady, a to především úsporou času. Dále by mělo docházet ke snižování nákladů na některé úředníky, kteří by v souladu s elektronizací byli nepotřební. Finanční úspora je spojená i s uchováváním agendy výhradně v elektronické formě. Elektronizace státní správy rovněž vede k transparentnosti procesů a rozhodování.

eGovernment vznikl v roce 1999 ve Velké Británii (adaptic, ©2012; Holešinský, 2009, s. 4).

1.2 Legislativa eGovernmentu

Zákon o eGovernmentu má za cíl nastavit podmínky, které budou vhodné pro elektronickou komunikaci, a to jak mezi občany a úřady, tak i mezi úřady navzájem, dále umožní, aby se spisy ve správních řízeních vedly v elektronické formě.

Za hlavní a nejpodstatnější právní normy upravující problematiku eGovernmentu v České republice lze označit následující zákony:

- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím
- Zákon o občanských průkazech č.328/1999 Sb.
- Zákon č. 29/2000 Sb., o poštovních službách
- Zákon č. 101/2000 Sb., o ochraně osobních údajů
- Zákon č. 227/2000 Sb., o elektronickém podpisu
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy
- Zákon č. 480/2004 Sb., o některých službách informační společnosti
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě
- Zákon č. 127/2005 Sb., o elektronických komunikacích

- Zákon č. 137/2006 Sb., o veřejných zakázkách
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů – též nazýván jako zákon o eGovernmentu nebo eGovernment Act
- Zákon č.301/2008 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o elektronických úkonech a autorizované konverzi dokumentů
- Zákon č.111/2009 Sb., o základních registrech (Štědroň, 2007, s. 18)

1.3 Vývoj eGovernmentu v České republice

První služba, kterou občané České republiky mohli vyřídit elektronicky prostřednictvím elektronické pošty, bylo v roce 1999 podávání žádostí o informace podle zákona o svobodném přístupu k informacím. Institut elektronického podpisu byl pak do českého právního řádu zaveden v roce 2000, avšak prováděcí předpis, který tuto funkci umožnil zavést do praxe, byl vydán až téměř půl roku poté. Elektronická komunikace tak byla umožněna v celé řadě agend, ale problémem byla nepřipravenost mnoha úřadů a neprovozování elektronických podatelen. Dále byl v roce 2000 zřízen Úřad pro veřejné informační systémy. Jeho úkolem byla koordinace informačních systémů veřejné správy tak, aby spolu mohly vzájemně komunikovat a vyměňovat si data. Dne 1.1.2003 tento úřad zanikl a jeho úlohu převzalo nově zřízené Ministerstvo informatiky. Přínosem Ministerstva bylo mimo jiné prosazení několika novel právních předpisů, např.: novela zákona o elektronickém podpisu (ta všem úřadům nařizovala provozovat elektronické podatelny a zavedla institut elektronické značky) nebo novela zákona o informačních systémech veřejné správy. Kromě oblasti legislativy spočívaly aktivity Ministerstva i v oblasti státní informační a komunikační politiky, Broadbandové strategii („broadband“ = vysokorychlostní nebo širokopásmové připojení, podle Ministerstva informatiky je broadband definován hranicí 256 kbit/s, hlavním cílem strategie bylo „dosažení penetrace broadbandu na úrovni 50% populace“) a Národní strategii informační bezpečnosti. Slabé postavení však Ministerstvo informatiky stavělo spíše do pozice marketingového propagátora eGovernmentu a monitorujícího subjektu problematiky eGovernmentu.

V roce 1999 se objevily první významné strategie, a to vládou nepříliš uznávaná Národní telekomunikační politika a Státní informační politika, se kterou už se vláda plně ztotožnila.

Odklon od původních ambiciózních strategických dokumentů přijatých v roce 1999 vedl v roce 2004 k přijetí Státní informační a komunikační politiky, která je též známa jako e-Česko 2006. Hlavní cíle, z nichž některé nebyly dosud dosaženy, byly např.:

1) Cíl vybavit postupně čipovými kartami vedoucí a odborné pracovníky veřejné správy
2) Cíl definovat, legislativně ošetřit a následně zavést do praxe jednotný bezvýznamový národní identifikátor
3) Cíl eliminovat na nejnižší možnou míru povinnost občana předkládat orgánům veřejné správy dokumenty v listinné podobě, pokud si je mohou orgány mezi sebou poskytovat elektronicky
4) Cíl připravit legislativní úpravu pravidel pro výměnu dat mezi orgány veřejné správy a postavení základních registrů veřejné správy a tento projekt uvést v život
5) Cíl používat elektronická tržiště v celé oblasti veřejné správy pro všechny druhy nákupů v ceně nad 100 000 Kč (MVČR, ©2008).

V návaznosti na tuto politiku vláda v roce 2005 přijala Národní politiku pro vysokorychlostní přístup „Broadband strategie ČR“ a Národní strategii informační bezpečnosti ČR.

Fungování Ministerstva informatiky trvalo do 31.5.2007, následně jeho úlohu převzalo částečně Ministerstvo pro místní rozvoj, Ministerstvo průmyslu a obchodu, projekt eGovernmentu převzalo Ministerstvo vnitra (Vaníček, 2011, s. 27-28).

1.4 eGovernment v zemích EU

V rámci Evropské unie působí při Evropské komisi organizace Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens (IDABC). Tato organizace monitoruje a podporuje informační a komunikační technologie. Pro vzájemné srovnání a hodnocení kvality eGovernmentu v členských zemích slouží údaje o vývoji služeb poskytovaných v rámci národního eGovernmentu. Sledování a hodnocení tohoto vývoje probíhá v rámci programu eGovernment Observatory. Kromě 27 členských států se tato kritéria sledují i u Chorvatska, Turecka, Norska, Islandu a Lichtenštejnska (EU+5).

Dokument, hodnotící stav v daném státě, má následující strukturu:

1) Profil země
2) Historie eGovernmentu
3) Strategie eGovernmentu
4) Legislativní rámec
5) Orgány podílející se na eGovernmentu
6) Kdo je kdo
7) Infrastruktura
8) Služby poskytované občanům a obchodním společnostem - v této části lze nalézt informace o stavu ke dni, kdy byla vložena data, sleduje se, kolik z 20 služeb, které by měly být v rámci eGovernmentu provozovány, je skutečně provozováno, a každá z těchto služeb je následně zařazena do jednoho ze stupňů, které popisují kvalitu služby (Budiš a Hřebíková, 2010, s. 19-21):

Stupeň	Název stupně	Popis
0	Nedostupné informace	Uživatelé nemají možnost nalézt o veřejné službě online informace
1	Informace	Uživatelé mají k dispozici online informace o veřejné službě
2	Interakce	Uživatelé mohou online stáhnout příslušné formuláře
3	Oboustranná interakce	Úřad provede zpracování online podaných formulářů včetně ověření identity
4	Úplné vyřízení	Případ může být zcela zpracován elektronicky včetně provádění plateb a rozhodnutí

Tabulka 1 – Stupně kvality služeb eGovernmentu (Budiš a Hřebíková, 2010, s. 20)

1.5 Systém eGovernmentu v České republice

1.5.1 Informační systémy veřejné správy

Informační systémy veřejné správy (ISVS) jsou vymezeny zákonem č. 365/2000 Sb., o informačních systémech veřejné správy, který je definuje jako soubor informačních systémů, které slouží pro výkon veřejné správy.

Za ISVS se považují všechny informační systémy uvedené v zákoně č. 365/2000 Sb. Za ISVS se považují informační systémy:

- o nichž zákon stanoví, že jde o ISVS
- jež nesou označení registr, rejstřík nebo evidence ze zákona
- jež jsou zákonem určeny bez označení ISVS
- jež zákon neupravuje, avšak orgán veřejné správy je využívá k výkonu činnosti

ISVS jsou spravovány orgány veřejné správy, na ISVS i na tyto orgány jsou kladeny následující požadavky:

1) Orgán veřejné správy musí uveřejňovat číselníky, pokud je jejich správcem; číselník lze definovat jako přípustné hodnoty datového prvku. Tvoří vždy dvojici kód-hodnota. Datový prvek je dále nedělitelný údaj v ISVS – např. jméno, pohlaví, telefonní číslo. Proto, aby se zamezilo nečitelnosti a nutnosti tato data převádět, jsou datové prvky standardizovány zákonem č.365/2000 Sb. Obdobně dochází ke standardizaci i u číselníků
2) Orgán veřejné správy musí MVČR v elektronické podobě a bez zbytečného odkladu zpřístupňovat informace o jím provozovaných ISVS; informace se zadávají do informačního systému o ISVS
3) Orgán veřejné správy musí zajistit, aby komunikace všech jeho ISVS probíhala přes referenční rozhraní a s využitím vyhlášených datových prvků; pouze u komunikujících ISVS (ty jsou zapsány v IS o ISVS)
4) Orgán veřejné správy musí dlouhodobě řídit své ISVS; daný orgán je zodpovědný za zpracování informační koncepce, v níž se uvádí charakteristika ISVS, které má orgán ve správě, jak jsou tyto ISVS financovány, správu ISVS a odpovědnost za ni, dlouhodobé cíle v řízení kvality a bezpečnosti ISVS
5) Orgán veřejné správy musí ke všem svým ISVS vést provozní dokumentaci; dokumentace obsahuje bezpečnostní politiku ISVS, bezpečnostní směrnice pro

činnost bezpečnostního správce, uživatelskou a systémovou příručku, podle povahy a rozsahu ISVS mohou být zahrnuty i jiné dokumenty (Lidinský et al., 2008, s. 12-17).

1.5.1.1 Czech POINT

Legislativně je Czech POINT vymezen opět zákonem č. 365/2000 Sb. Jeho označení je zkrácený název pro Český podací ověřovací informační národní terminál. Jeho účelem je sloužit jako kontaktní místo výkonu veřejné správy, čímž má dojít ke snížení zatížení občana při vyřizování agendy. Kontaktní místa se nacházejí na pobočkách České pošty, vybraných zastupitelských úřadech a dalších institucích.

Pracoviště Czech POINT občanům poskytují:

- výpis z Katastru nemovitostí
- výpis z Obchodního rejstříku
- výpis z Živnostenského rejstříku
- výpis z Rejstříku trestů
- přijetí podání podle živnostenského zákona
- žádost o výpis nebo opis z Rejstříku trestů podle zákona č. 124/2008 Sb.
- výpis z bodového hodnocení řidiče
- vydání ověřeného výstupu ze Seznamu kvalifikovaných dodavatelů
- podání do registru účastníků provozu modulu autovraků ISOH
- výpis z insolvenčního rejstříku
- datové schránky
- autorizovaná konverze dokumentů na žádost
- centrální úložiště ověřovacích doložek (v němž jsou evidovány všechny ověřovací doložky k autorizované konverzi dokumentů)
- úschovna systému Czech POINT (jsou v ní dočasně uloženy všechny dokumenty ze všech pracovišť Czech POINTU pro konverzi)
- CzechPOINT@office (část systému určená pro některé subjekty veřejné správy v rámci výkonu jejich působnosti)

- Czech POINT E-SHOP – výpisy poštou (možnost objednat si výpis z Obchodního rejstříku, Živnostenského rejstříku nebo z Katastru nemovitostí pomocí webového formuláře, tyto jsou následně do tří pracovních dnů doručeny poštou) (Lidinský et al., 2008, s. 17; MVČR, ©2012).

1.5.2 Základní registry veřejné správy

Základní registry jsou důležitým prvkem, který napomůže rozvoji eGovernmentu v České republice. Jejich účel je, aby úřady mohly sdílet data. Ta budou moci být ze strany úředníků považována za důvěryhodná, a odpadne tak nutnost je ověřovat, zároveň nebude třeba tato data úřadům sdělovat pokaždé, kdy budou potřebná (Holešinský, 2009, s. 5-6).

Vytvoření centrálních registrů veřejné správy, které by řešily dosavadní potíže související s nejednotností, multiplicitou a neaktuálností klíčových databází, je jedním z pilířů elektronizace veřejné správy.

Zásadním krokem k fungování systému základních registrů bylo přijetí zákona č. 111/2009 Sb., o základních registrech a zákona č. 227/2009 Sb. na počátku roku 2009. Tyto zákony vytvářejí předpoklad pro spuštění systému od 1. 7. 2010 ve zkušebním provozu a o rok později v ostrém provozu (MVČR, ©2010).

Pozitivem zákona o základních registrech je roztřídění vedených údajů na:

1) Referenční údaje – ty jsou vymezeny zvláštním zákonem, budou se uchovávat pouze v jednom centrálním základním registru a další registry tyto údaje budou pouze přebírat
2) Referované údaje – jsou vedeny v ISVS a jsou referenční v základním registru
3) Ostatní údaje – nemusejí být přebírány ze základních registrů (Lidinský et al., 2008, s. 77).

Základní registry jsou celkem čtyři:

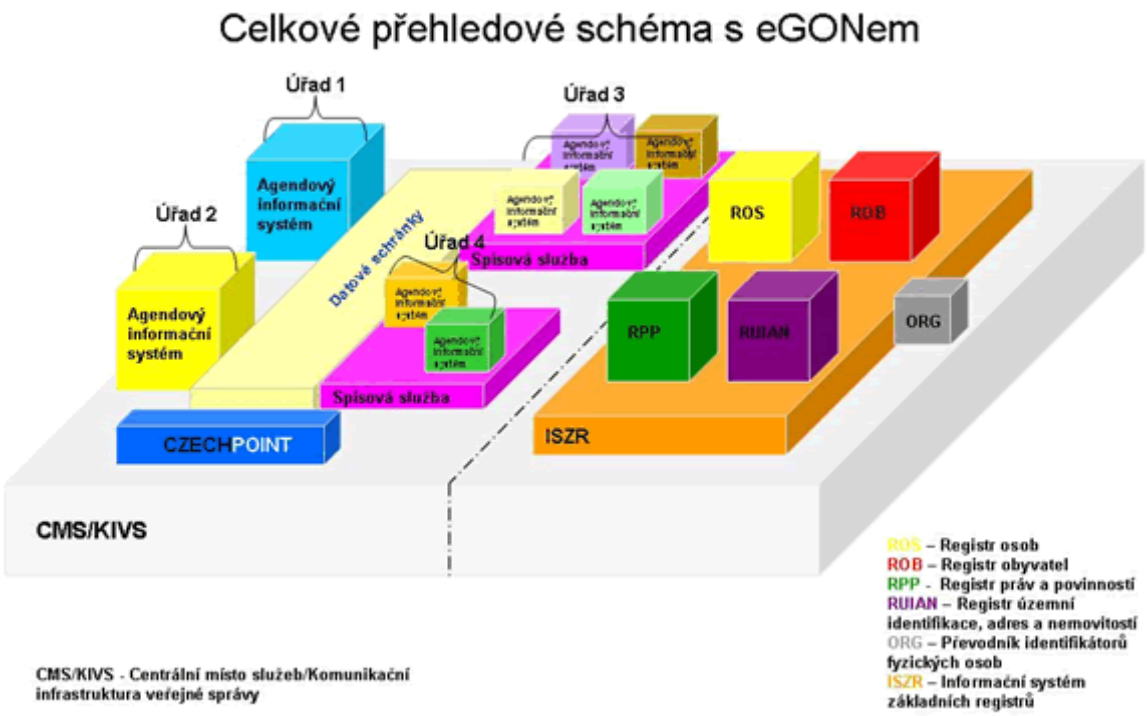
1) Registr obyvatel obsahující základní údaje o občanech a cizincích s povolením k pobytu, mezi tyto údaje patří: jméno a příjmení, datum a místo narození a úmrtí a státní občanství obsahující základní údaje o občanech a cizincích s povolením k pobytu, mezi tyto údaje patří: jméno a příjmení, datum a místo narození a úmrtí a státní občanství

2) Registr práv a povinností obsahující referenční údaje o působnosti orgánů veřejné moci, mj. oprávnění k přístupu do k jednotlivým údajům, informace o změnách v těchto údajích apod. - slouží jako garance bezpečné správy dat občanů a subjektů vedených v jednotlivých registrech

3) Registr osob obsahující údaje o právnických osobách, podnikajících fyzických osobách, orgánech veřejné moci i o nekomerčních subjektech, jako jsou občanská sdružení a církve

4) Registr územní identifikace, adres a nemovitostí spravující údaje o základních územních a správních prvcích

Schéma fungování základních registrů:



Obrázek 1 – Schéma fungování základních registrů (MVČR, ©2010)

1.5.3 Elektronický podpis

Klíčovým se stal zákon č. 227/2000 Sb., o elektronickém podpisu, který nabyl účinnosti 1.10.2000. Ten tvoří legislativní rámec pro použití a zrovnoprávňuje elektronický podpis s vlastnoručním. Elektronický podpis upravují následující právní normy a standardy:

- Směrnice 1999/93/EC Evropského parlamentu a Rady Evropské unie o zásadách Společenství pro elektronické podpisy
- Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů
- Zákon č. 226/2002 Sb. (jde o novelu zákona č. 227/2000 Sb.)
- Vyhláška č. 366/2001 Sb., o upřesnění podmínek stanovených v zákoně o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu.

Mezi hlavní výhody elektronického podpisu lze zařadit to, že příjemce zprávy s jistotou zná autora či odesílatele, že během přenosu zprávy nedošlo k žádným úpravám (ověření integrity zprávy), že je naprosto vylučitelné, že by odesílatel prohlásil, že zprávu neodeslal (nepopiratelnost zprávy) a že není možná napodobitelnost podpisu (CzechTrade, ©2011).

1.5.3.1 Realizace elektronického podpisu

Z uživatelského hlediska je podpis elektronického dokumentu snadný, uživatel pouze vybere daný dokument a vydá příkaz. Za celý průběh pak odpovídá speciální software.

Ke vzniku elektronického podpisu dochází vypočtením hashe, tedy otisku dokumentu, který je následně zašifrován privátním klíčem. Dochází tak k vytvoření elektronického podpisu a jeho následnému přiložení k dokumentu. Příjemce dokumentu obdrží nezašifrovanou, původní verzi dokumentu, elektronický podpis a certifikát. U dokumentu se znovu vypočte hash a odšifruje elektronický podpis. Tímto dostane příjemce původní otisk a následným porovnáním obou otisků se zjistí, jestli nedošlo k pozměnění dokumentu (CzechTrade, ©2011).

1.5.3.2 Zaručený elektronický podpis

Může nastat případ, kdy je třeba použít podpis založen na certifikátu. Pro každou podepsanou zprávu je pak elektronický podpis jiný právě v závislosti na konkrétní zprávě. Certifikát vydává poskytovatel certifikačních služeb, certifikační autorita. Přehled těchto poskytovatelů je uveřejněn ve Věstníku Úřadu pro ochranu osobních údajů, v současnosti v České republice působí tři subjekty – První certifikační autorita, a.s., eIdentity, a.s. a PostSignum QCA (CzechTrade, ©2011).

1.5.4 Systém OPEN

Název je odvozen od počátečních písmen slov Online Procedures Enhancement for Civil Applications (Zlepšení online vyřizování žádostí občanů).

Systém OPEN, neboli on-line úřad, se vyznačuje spoluprací úřadu s občanem za využití internetu. Přínosem je úspora času, peněz, ale i materiálu (papír). Systém OPEN má také vést k odbourání korupce a ke stejnému jednání se všemi občany. Občan má možnost se nejen online informovat o tom, v jakém stádiu je vyřizování jeho žádosti, ale i o stavu žádostí ostatních občanů. Zjistit tak lze třeba to, který úředník má žádost na starost, jakou dobu už žádost má a datum, kdy se očekává její vyřízení (Štědroň, 2007, s. 67).

1.5.5 Elektronické volby

Známy též jako e-volby či e-voting. Většinou se tímto označením myslí realizace aktivního volebního práva prostřednictvím internetu.

Hlavními výhodami tohoto způsobu konání voleb by mohly být zejména:

- vyšší účast voličů (potenciálně) – pro účast ve volbách není třeba se nacházet v místě trvalého bydliště nebo návštěva volební místnosti

- rychlejší získání výsledků – díky počítačovým technologiím jsou hlasy nejen rychleji sečteny a vyhodnoceny, ale dochází i k eliminaci rizika chyby a netransparentnosti

- úspora finančních prostředků – není potřeba tisk volebních lístků ani jejich doručení voličům

Na druhou stranu jako hlavní nevýhody lze zmínit:

- nebezpečnost – otázka zneužití počítače voliče jinou osobou, problematika počítačových virů, přetížení serverů

- zvýšení účasti voličů jen mírně a krátkodobě

- nejedná se o přímou volbu – rozpor s požadavkem v Ústavě

- existence rizika kupčení s hlasy (Štědroň, 2007, s. 70-71).

1.5.6 Datové schránky

Podrobněji se tato práce problematice datových schránek věnuje níže

1.5.7 Další elektronické aplikace a rozhraní veřejné správy

1.5.7.1 Elektronická aplikace pro „whistleblowing“

Jedná se o možnost upozornit na korupci a jiné nekalé jednání jiným způsobem než upozornit nadřízeného či policii (Štědroň, 2007, s. 68).

1.5.7.2 Elektronické tržiště

Tento systém umožňuje, aby i zakázky malého rozsahu byly zadávány systémem, který požaduje zákon č. 40/2004 Sb., o veřejných zakázkách, tedy zakázky do dvou milionů korun bez DPH zadávat transparentním a nediskriminačním způsobem a za cenu obvyklou v místě a čase zadání (Štědroň, 2007, s. 69).

1.5.7.3 Opencard – elektronická peněženka

Jedná se o chytrou čipovou kartu pro obyvatele Prahy a její návštěvníky. Kartu vydává Magistrát hl. m. Prahy, za cíl si klade snadný přístup ke službám nabízeným městem.

V současnosti má karta široké využití – funguje jako průkazka v Pražské integrované dopravě, držitel má nárok na slevu 5-50% u vybraných organizací a partnerů, lze ji použít k bezhotovostní úhradě parkovného ve vybraných městských částech, karta je přijímána jako čtenářský průkaz v pobočkách Městské knihovny v Praze a aplikace Vím jak řídím uživateli po registraci na portálu města Prahy nabízí přehled jeho nevyřešených dopravních přestupků na území hl. m. Prahy (Magistrát hl. m. Prahy, ©2010a; ©2010b).

2 INFORMAČNÍ SYSTÉM DATOVÝCH SCHRÁNEK

2.1 Co je datová schránka

Datová schránka slouží k elektronické komunikaci v eGovernmentu. Je to elektronické úložiště, které slouží zejména k doručování orgány veřejné moci, provádění úkonů vůči orgánům veřejné moci a dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob. Provoz funkcí datové schránky je zajištěn informačním systémem datových schránek. Jeho správa je zcela v kompetencích Ministerstva vnitra, provozovatelem je držitel poštovní licence – Česká pošta, s. p. Podle zákona č. 300/2008 Sb. existují 4 typy datových schránek, a to podle subjektů, pro které jsou schránky zřízeny, tedy:

- DS orgánů veřejné moci
- DS právnických osob
- DS fyzických osob
- DS podnikajících fyzických osob

2.2 Pojmy z oblasti datových schránek

2.2.1 Datová zpráva

Datová zpráva je forma, kterou má každý dokument dodávaný či doručovaný datovou schránkou. Datová zpráva je definována zákonem o elektronickém podpisu jako elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích používaných při zpracování a přenosu dat elektronickou formou.

Datová zpráva se skládá z obálky a obsahu, jehož součástí může být jedna nebo i více příloh. Velikost datové zprávy však nesmí přesáhnout 10 MB (Budiš a Hřebíková, 2010, s. 91).

2.2.2 Datový formát

Pojmem datový formát se rozumí, jakým způsobem je dokument kódován. Mezi datové formáty patří například HTML, PDF, PDF/A, TXT nebo XML. Proto, aby datová zpráva mohla být přijata, musí mít přípustný formát a velikost (Budiš a Hřebíková, 2010, s. 91-92).

2.2.3 Poštovní datová zpráva

Tato služba umožňuje zasílání datových zpráv vzájemně mezi datovými schránkami fyzických, podnikajících fyzických a právnických osob (Česká pošta, ©2011).

2.2.4 Časové razítko

Časové razítko vydává certifikační autorita a slouží k tomu, aby bylo možné prokázat přesný čas, kdy byl dokument vytvořen. Používá se v kombinaci s elektronickým podpisem, který prokazuje identitu, časové razítko pak prokazuje čas vytvoření dokumentu (Budiš a Hřebíková, 2010, s. 95).

2.2.5 Autorizovaná konverze dokumentů

Autorizovaná konverze dokumentů je zákonem č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů:

- úplné převedení dokumentu v listinné podobě do dokumentu obsaženého v datové zprávě, ověření shody obsahu těchto dokumentů a připojení ověřovací doložky

- úplné převedení dokumentu obsaženého v datové zprávě do dokumentu v listinné podobě a ověření shody obsahu těchto dokumentů a připojení ověřovací doložky

Jedná se tedy o situaci, kdy máme k dispozici dokument v listinné podobě a potřebujeme jej převést do elektronické formy, která však musí být oficiálně uznatelná, nebo naopak o převedení elektronického dokumentu na listinný. Takto vzniklý dokument má co do právních účinků stejnou sílu jako ten, ze kterého se převáděl. Při každé konverzi se k dokumentu připojuje ověřovací doložka, která se zároveň ukládá do centrálního úložiště ověřovacích doložek.

Výstup konverze je podle toho, pro co se rozhodne, zákazníkovi předán na CD nebo DVD nebo je mu zaslán do Úschovny. Úschovna je úložiště, kde jsou konvertované dokumenty uloženy do doby, než jsou zákazníky vyzvednuty (MVČR, ©2012).

2.2.5.1 Autorizovaná konverze na žádost

Tento typ konverze je určen pro občany a provádí se na kontaktních místech veřejné správy. Úředník provádějící konverzi má k dispozici formulářové rozhraní, ve kterém po jednotlivých krocích prochází procesem autorizované konverze – scanování dokumentu,

kontrola, vytvoření ověřovací doložky, uložení v Centrální evidenci ověřovacích doložek (MVČR, ©2012).

2.2.5.2 Autorizovaná konverze z moci úřední

Tento typ konverze slouží pro převádění listinných dokumentů na elektronické a naopak, a to těch dokumentů, které se nacházejí ve vlastnictví úřadu. Konverzi z moci úřední mohou provádět pouze orgány veřejné moci.

Pro konverzi z moci úřední existuje také speciální rozhraní, CzechPOINT@office, které obsahuje nejen formulářové rozhraní pro autorizovanou konverzi z moci úřední, ale také rozhraní pro výpis/opis z Rejstříku trestů (MVČR, ©2012).

2.2.5.3 Bezpečnostní prvky konvertovaného dokumentu

Při konvertování dokumentů je nutné identifikovat a zaznamenat bezpečnostní prvky, kterými se dokument před převedením vyznačoval. Sledují se následující znaky:

1) plastický text
    - a to nejen plastický ve smyslu prostorového, hmatově vnímatelného zobrazení, ale i ve smyslu digitálního zpracování
2) vodoznak
    - slouží k ochraně dokumentu před pozměněním a k ochraně práv jeho autora
    - obsahuje dodatečně vložené informace v digitální či analogové formě
    - viditelný vodoznak – dokument je opatřen viditelnou značkou, kterou je obtížné odstranit
    - autentizační bitový vzor (skrytý vodoznak) – součást digitálních dokumentů
3) reliéfní tisk
    - je grafickým zpracováním hmotného nosiče, kdy vzniká vytlačováním matrice do tohoto hmotného nosiče, a to zpravidla s využitím tepla a tlaku

4) embossing

   - jedná se o metodu podobnou reliéfnímu tisku, která navíc umožňuje použít i barvy
   - tato metoda se dá použít například u fólie, ve které může být vytlačen určitý motiv

5) suchá pečeť

   - tato technika slouží k vytvoření „razítka, “ které má zabránit padělání a pozměňování dokumentů
   - vzniká trojrozměrný efekt viditelný z obou stran dokumentu

6) reliéfní ražba

   - obdoba suché pečeti

7) optický variabilní prvek

   - tento prvek má zabránit, aby byl dokument barevně kopírován
   - v praxi se nejčastěji lze setkat s holografickými laminačními fóliemi, které prodlužují stabilitu optických vlastností dokumentu

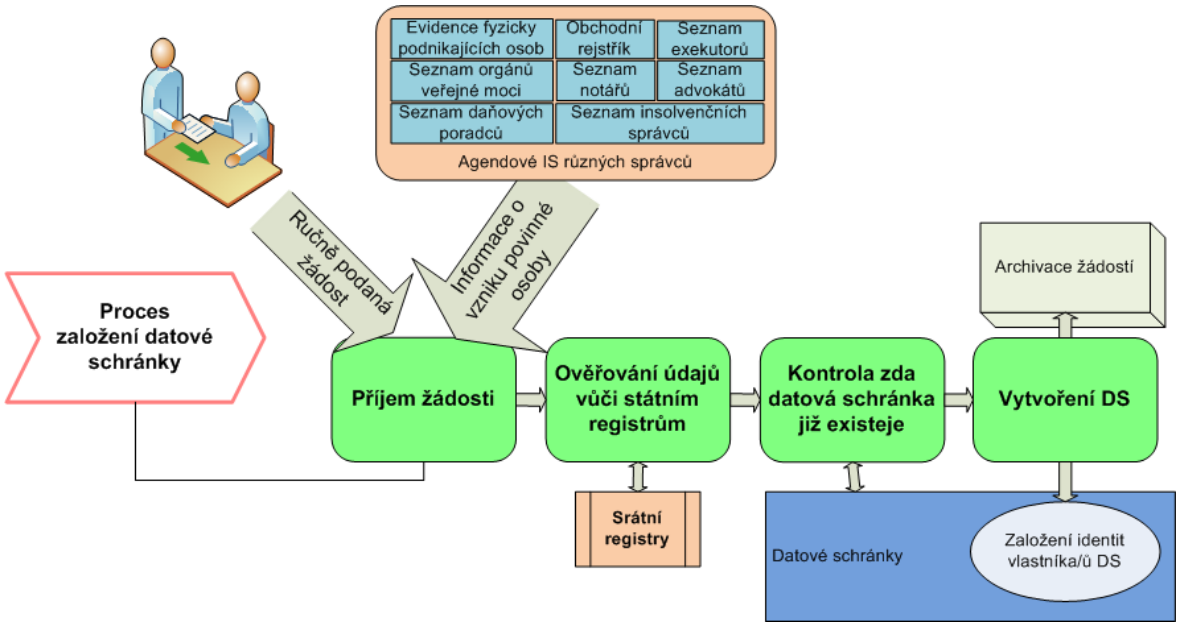
Podle zákona č. 300/2008 Sb. se nesmějí konvertovat dokumenty, u kterých konverze nenahrazuje jejich jedinečnost, tedy: občanské průkazy, cestovní doklady, zbrojní průkazy, řidičské průkazy, vojenské knížky, služební průkazy, průkazy o povolení k pobytu cizinců, rybářské lístky, lovecké lístky, vkladní knížky, šeky, směnky nebo jiné cenné papíry, losy, sázenky, geometrické plány, rysy a technické kresby.

Při autorizované konverzi dokumentu, jenž má více než 150 stran, se hovoří o rozsáhlé konverzi dokumentů. Z časových a prostorových nároků na takovou konverzi se provádí jen na specializovaných pracovištích s potřebným vybavením.

Při konverzi z listinné do elektronické podoby dokumentu je poplatek za každou stranu 30 Kč (MVČR, ©2012).

2.3 Zřízení datové schránky

Datovou schránku lze založit dvěma způsoby – ze zákona nebo na žádost. Ze zákona se datové schránky zřizují orgánům veřejné moci, právnickým osobám zřízeným zákonem, právnickým osobám zapsaným v obchodním rejstříku, organizačním složkám podniků zahraničních právnických osob zapsaným v obchodním rejstříku, insolvenčním správcům, advokátům a daňovým poradcům. Žádost o zřízení datové schránky mohou podat fyzické osoby, většina podnikajících fyzických osob a některé právnické osoby (občanská sdružení, církve…), dále může žádost o zřízení další datové schránky podat i orgán veřejné moci (Budiš a Hřebíková, 2010, s. 121).



Obrázek 2 – Proces založení datové schránky (Stiegler, ©2009)

2.3.1 Zřízení datové schránky ze zákona

U subjektů, kterým je datová schránka zřízena ze zákona, došlo k jejímu zřízení do 90 dnů ode dne účinnosti zákona 300/2008 Sb., tedy do 28.9.2009, advokátů a daňovým poradcům pak schránka bude založena 1.7.2012. Pokud však datovou schránku tyto subjekty chtějí využívat již dříve, mají možnost si podat žádost jako podnikající fyzické osoby. Datová schránka subjektu, který vznikl po 1.7.2009, je zřízena bezodkladně po jeho vzniku u orgánu veřejné moci, u ostatních bezodkladně poté, co Ministerstvo vnitra obdrží informaci o jejich zapsání do zákonem stanovené evidence (Budiš a Hřebíková, 2010, s. 121-122).

2.3.2 Zřízení datové schránky na žádost

Žádost o zřízení datové schránky lze podat:

– osobně na podatelně Ministerstva vnitra nebo na kontaktních místech veřejné správy (Czech POINT)

- poštou

- elektronickou poštou na adrese elektronické podatelny Ministerstva vnitra (posta@mvcr.cz)

- v případě, že podává orgán veřejné moci žádost o zřízení další datové schránky, může tak učinit prostřednictvím již existující datové schránky

Formulář žádosti o zřízení datové schránky je dostupný na adrese www.datoveschranky.info. V případě osobního podání žádosti je nutné, aby obsahovala úředně ověřený podpis žadatele. Tato podmínka však neplatí při podpisu žádosti před zaměstnancem Ministerstva vnitra nebo kontaktního místa veřejné správy. U elektronického podání není ověření podpisu nutné, obsahuje-li žádost uznávaný elektronicky podpis.

Způsob podání žádosti je jen na volbě žadatele. Může zvolit poštovní zaslání úředně ověřené žádosti na Ministerstvo vnitra, elektronické podání v programu Software602 Form Filler a další výše zmíněné. Asi nejjednodušší a nejrychlejší se jeví podání žádosti na některém z kontaktních míst veřejné správy. Zde je možné žádost podat od 1.7.2009. Úředník žádost ihned na místě žádost ověří a žadatel do tří pracovních dnů obdrží přístupové údaje k datové schránce (moje zkušenost bylo obdržení údajů zhruba do jedné hodiny) (Budiš a Hřebíková, 2010, s. 122-125; Holešinský, 2009, s. 9).

2.3.2.1 Žádost u fyzických osob

Ke zřízení dochází bezplatně do 3 pracovních dnů od podání žádosti.

Náležitosti:

- jméno, popřípadě jména, příjmení, jejich případné změny
- rodné příjmení
- den, měsíc a rok narození
- místo a okres narození; pokud se fyzická osoba narodila v cizině, místo narození a stát, na jehož území se narodila
- státní občanství, není-li fyzická osoba státním občanem ČR

žádost musí obsahovat úředně ověřený podpis fyzické osoby (MVČR, ©2011). Vzor žádosti – příloha P I

2.3.2.2 Žádost u podnikajících fyzických osob

Ke zřízení dochází bezplatně do tří dnů od podání žádosti.

Kromě údajů stejných jako u žádosti fyzické osoby musí žádost podnikající fyzické osoby navíc obsahovat:

- identifikační číslo ekonomického subjektu (IČO), bylo-li přiděleno
- místo podnikání, popřípadě sídlo (MVČR, ©2011). Vzor žádosti – příloha P II

2.3.2.3 Žádost u právnických osob

Právnickým osobám, kterým není datová schránka zřízena automaticky, je datová schránka zřízena bezplatně do tří dnů od podání žádosti.

Náležitosti žádosti:

- název nebo obchodní firma
- identifikační číslo ekonomického subjektu, a nebylo-li přiděleno, registrační číslo, evidenční číslo nebo jiný obdobný údaj, byl-li přidělen
- adresa sídla
- jméno, popřípadě jména, příjmení, datum narození a adresa pobytu osoby oprávněné jednat jménem právnické osoby
- stát registrace nebo evidence právnické osoby
- žádost o zřízení datové schránky právnické osoby musí obsahovat úředně ověřený podpis osoby oprávněné jednat jménem právnické osoby (MVČR, ©2011). Vzor žádosti – příloha P III

2.3.2.4 Žádost u orgánů veřejné moci

Další datové schránky orgánu veřejné moci zřídí ministerstvo orgánu veřejné moci bezplatně na žádost tohoto orgánu do 3 pracovních dnů ode dne podání žádosti. Další datová schránka se zřizuje zejména pro potřeby vnitřní organizační jednotky orgánu veřejné moci.

Náležitosti žádosti o zřízení další datové schránky orgánu veřejné moci:

- název orgánu veřejné moci a název vnitřní organizační jednotky orgánu veřejné moci, pro jejíž potřebu se datová schránka zřizuje
- identifikační číslo ekonomického subjektu, bylo-li přiděleno
- adresa
- jméno, případně jména, příjmení, datum narození a adresa pobytu osoby, jíž mají být zaslány přístupové údaje

Splňuje-li žádost o zřízení další datové schránky orgánu veřejné moci tyto požadavky, zřídí ministerstvo další datovou schránku orgánu veřejné moci a zašle přístupové údaje k této datové schránce osobě uvedené v žádosti do vlastních rukou, jinak orgán veřejné moci po předchozí marné výzvě k odstranění nedostatků žádosti vyrozumí o tom, že další datovou schránku orgánu veřejné moci nelze zřídit.

Orgánu veřejné moci se zřizuje pouze datová schránka orgánu veřejné moci (MVČR, ©2011).

2.4 Zpřístupnění datové schránky

Zpřístupnění datové schránky je nezbytné pro odesílání a přijímání datových zpráv. Ke zpřístupnění dochází v okamžiku, kdy se oprávněná osoba poprvé přihlásí údaji, které jí zašle Ministerstvo vnitra. V případě, že se oprávněná osoba do 15 dnů od doručení údajů nepřihlásí, je datová schránka zpřístupněna automaticky (Budiš a Hřebíková, 2010, s. 125-126; MVČR, ©2011).

2.5 Znepřístupnění datové schránky

Dočasně znepřístupnit datovou schránku může Ministerstvo vnitra na základě žádosti osoby, které byla datová schránka zřízena. Znepřístupnění proběhne do tří pracovních dnů ode dne podání žádosti. Její opětovné zpřístupnění se provede opět na žádost do tří pracovních dní. Datovou schránku lze na žádost znepřístupnit dvakrát za rok, poté je další znepřístupnění možné po uplynutí nejméně jednoho roku od posledního zpřístupnění. Subjekty, jimž je datová schránka zřízena ze zákona, nemají nárok podat žádost o znepřístupnění datové schránky.

Ze zákona musí Ministerstvo vnitra datovou schránku znepřístupnit v případě, že se k fyzické nebo podnikající fyzické osobě váží tyto události: úmrtí, prohlášení za mrtvého, zbavení nebo omezení způsobilosti k právním úkonům, omezení osobní svobody z důvodu vzetí do vazby, výkonu trestu odnětí svobody, výkonu zabezpečovací detence, ochranného

léčení nebo ochrany zdraví lidu. Den, kdy k dané události došlo, je i dnem, ke kterému je datová schránka znepřístupněna. U právnických a podnikajících fyzických osob dochází ke znepřístupnění dnem, kdy došlo k výmazu osoby ze zákonem stanovené evidence. U právnických osob, jimž je datová schránka zřízena ze zákona, a u orgánů veřejné moci dochází ke znepřístupnění dnem zrušení subjektu (Budiš a Hřebíková, 2010, s. 126-127; Holešinský, 2009, s. 12).

2.6 Zrušení datové schránky

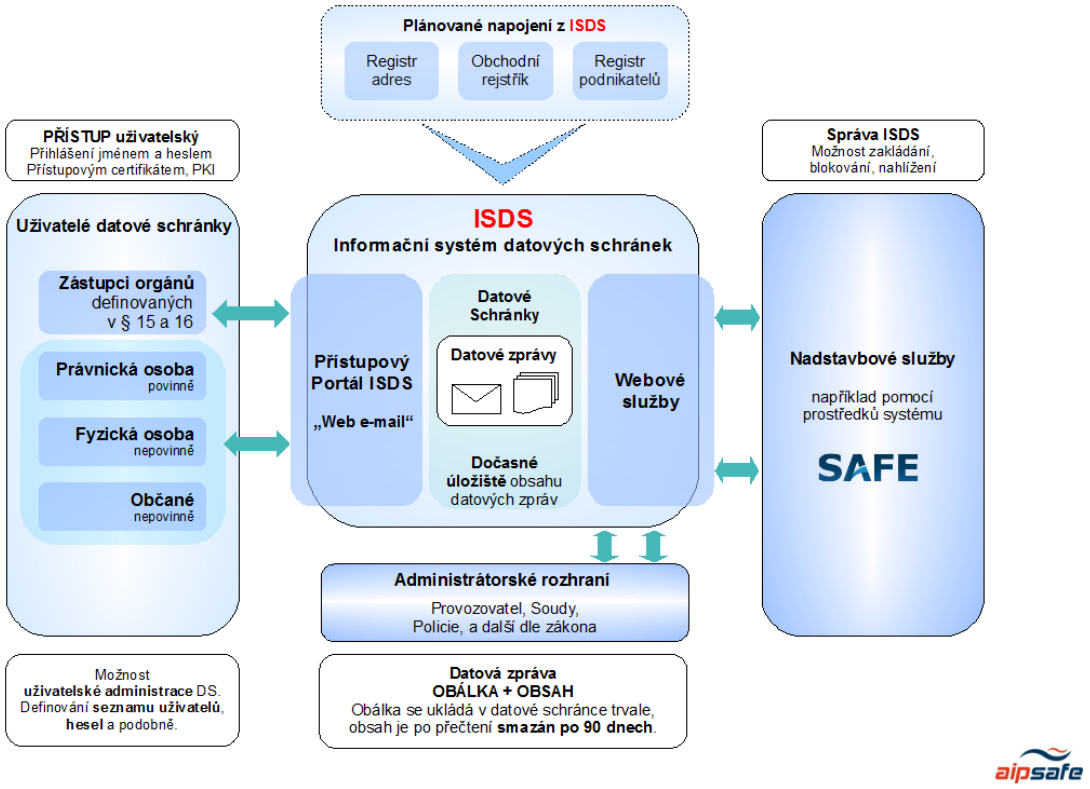
Zrušit datovou schránku lze pouze po jejím předchozím znepřístupnění. Zrušení nastává v těchto případech:

- u fyzické osoby po uplynutí tří let ode dne úmrtí
- u podnikající fyzické osoby po uplynutí tří let ode dne výmazu ze zákonem stanovené evidence
- u právnické osoby po uplynutí tří let ode dne zániku
- u orgánu veřejné moci po uplynutí tří let ode dne zrušení

Během této tříleté lhůty je sice datová schránka znepřístupněna, ale její obsah je uchován. Pokud má právnická osoba, která zanikne, právního nástupce, její datová schránka sice bude znepřístupněna, ale ne zrušena. Právní nástupce má pak umožněn přístup k obsahu datové schránky této zaniklé právnické osoby. Datovou schránku nelze zrušit na žádost (Budiš a Hřebíková, 2010, s. 127-128).

2.7 Informační systém datových schránek

ISDS je informačním systémem, který obsahuje informace o datových schránkách a o jejich uživatelích. Byl vytvořen, aby zajišťoval provoz elektronické komunikace mezi fyzickými, podnikajícími fyzickými a právnickými osobami na straně jedné a orgány veřejné moci na straně druhé a mezi orgány veřejné moci vzájemně. Jeho správcem je Ministerstvo vnitra a provozovatelem Česká pošta, a.s. (AiP Safe, ©2009).



Obrázek 3 – Datové schránky v prostředí informačních systémů (AiP Safe, ©2009)

Při odesílání dokumentu z datové schránky fyzické, podnikající fyzické nebo právnické osoby do datové schránky jiné fyzické, podnikající fyzické nebo právnické osoby je odesílatel dokumentu povinen za toto odeslání uhradit provozovateli ISDS odměnu. Ta je ve výši 15,04 Kč bez DPH za jednu datovou zprávu, avšak celková výše se odvíjí od počtu odeslaných zpráv za daný kalendářní měsíc. Provozovatel, tedy Česká pošta, a.s., stanovil měsíční poplatky podle celkového počtu odeslaných zpoplatněných zpráv, a to (Budiš a Hřebíková, 2010, s. 142-143):

Počet odeslaných datových zpráv v kalendářním měsíci	Cena (bez DPH)
1-10	50 Kč
11-50	35 Kč
Více než 50	20 Kč

Tabulka 2 – Měsíční poplatky za datové zprávy (Budiš a Hřebíková, 2010, s. 143)

2.7.1 Údaje v ISDS

Údaje vedené v ISDS slouží správci jako evidence údajů, které mají vztah ke zřízení a provozování datových schránek. Všechny údaje v ISDS jsou neveřejné a nelze je poskytnout třetím osobám. Výjimku tvoří pouze kontaktní adresa, na kterou má být adresátu doručováno, a to tehdy, byl-li dán souhlas k jejímu uveřejnění.

Pomocí údajů v ISDS plní Ministerstvo vnitra svou povinnost umožnit identifikovat datovou schránku, do níž je tak možno doručovat. Datová schránka je identifikována pomocí identifikátoru (Budiš a Hřebíková, 2010, s. 145-148).

3 PROCES IMPLEMENTACE DATOVÝCH SCHRÁNEK V ČESKÉ ELEKTRONICKÉ VEŘEJNÉ SPRÁVĚ

3.1 Rok 2000

V roce 2000 byl založen Úřad pro veřejné informační systémy, který měl odpovědnost za strategické plánování v oblasti informačních systémů veřejné správy. V tomto roce byl také schválen zákon o veřejných informačních systémech a byla přijata první verze Akčního plánu pro realizaci státní informační politiky (MUNI, ©2010).

3.2 Rok 2001

V tomto roce dochází k připojení České republiky k akčnímu plánu eEurope+, který se zaměřuje na podporu rozvoje informační společnosti v členských státech (MUNI, ©2010).

3.3 Rok 2003

Založeno Ministerstvo informatiky, jehož úkolem bylo mimo jiné zajistit koordinaci a rozvoj v oblasti elektronizace veřejné správy.

V roce 2003 byl spuštěn portál veřejné správy portal.gov.cz(pilotně) (MUNI, ©2010).

3.4 Rok 2004

Přijata státní informační a komunikační politika eCzech 2006.

Plnohodnotné fungování portálu veřejné správy (MUNI, ©2010).

3.5 Rok 2005

Přijata státní strategie pro informační ochranu a soukromí.

Od roku 2005 mají instituce veřejné správy povinnost provozovat elektronické podatelny, tedy zabezpečené emailové systémy, jejichž prostřednictvím dochází k výměně digitálně podepsaných dokumentů mezi institucemi a uživateli (MUNI, ©2010).

3.6 Rok 2006

V roce 2006 se v české elektronické veřejné správě zavádí elektronický podpis a eStamp autentizační služba (MUNI, ©2010).

3.7 Rok 2007

V roce 2007 vzniká Vládní rada pro informační společnost a zaniká Ministerstvo informatiky. Vedení eGovernmentu a informační společnosti je svěřeno Ministerstvu vnitra (MUNI, ©2010).

3.8 Rok 2008

Provoz kontaktních míst veřejné správy, Czech POINT, je zahájen v lednu 2008, a občané tak nemusejí navštěvovat několik úřadů při vyřizování jedné záležitosti, přístup k veřejným záznamům jim umožňují one-stop body.

Dne 17.7.2008 je přijat zákon o elektronických akcích a povolených konverzích dokumentů, Český eGovernment Act (MUNI, ©2010).

3.9 Rok 2009

V únoru tohoto roku dochází k podpisu smlouvy o provozování informačního systému Datové schránky mezi generálním ředitelem České pošty a ministrem vnitra. Provozování datových schránek má být spuštěno 1.7.2009.

Zákon o základních registrech byl prezidentem podepsán v dubnu 2009, který vstoupil v platnost 1.7.2010.

Pro zájemce a budoucí uživatele datových schránek byla v červnu 2009 spuštěna demo-verze datových schránek, která byla určena pro jejich seznámení se se systémem.

Hlavní úlohy Czech POINTU byly od července 2009 zejména konverze listinných dokumentů do elektronické formy, zpracovávání žádostí o zřízení datových schránek a dalších žádostí (zpřístupnění/znepřístupnění DS).

V platnost vstupuje zákon o elektronických akcích a povolené konverzi dokumentů, a zrovnoprávňuje tak listinné a elektronické dokumenty. Navíc ukládá povinnost orgánům veřejné správy a právnickým osobám zapsaným v Obchodním rejstříku, aby mezi sebou komunikovaly prostřednictvím datových schránek.

Ministerstvo vnitra svoji datovou schránku aktivovalo v září roku 2009.

V polovině října již bylo evidováno přes 350 000 datových schránek, z nichž necelých 8 000 byly datové schránky orgánů veřejné správy, 340 000 DS právnických osob a přes 14 600 DS patřilo jiným než právnickým osobám. Aktivováno bylo 554 700 DS.

Plný provoz datových schránek začal 1.11.2009, do kdy také podle zákona všechny právnické osoby a orgány veřejné správy měly povinnost svou datovou schránku aktivovat (MUNI, ©2010).

PRAKTICKÁ ČÁST

4 ANALÝZA VYUŽITÍ DATOVÝCH SCHRÁNEK V ČESKÉ REPUBLICE ORGÁNY VEŘEJNÉ MOCI, PRÁVNICKÝMI OSOBAMI A OSTATNÍMI

Jak již bylo uvedeno výše, v České republice jsou datové schránky zřizovány ze zákona pro orgány veřejné správy, právnické osoby zapsané v Obchodním rejstříku, organizační složky podniků zahraničních právnických osob zapsaných v Obchodním rejstříku, insolvenční správce, advokáty a daňové poradce, nebo na základě žádosti, a to pro fyzické osoby a některé právnické osoby, žádost o zřízení jedné či více dalších datových schránek může rovněž podat orgán veřejné správy. Tato kapitola se pak zabývá různými oblastmi využití datových schránek těmito subjekty.

4.1 Počet datových schránek

Na internetové adrese http://www.datoveschranky.info/ jsou dostupné základní statistiky o aktuálním počtu datových schránek, počtu odeslaných zpráv a o úspěšnosti doručení přihlášením, dále je možno zde najít graficky znázorněný vývoj počtu datových schránek a počet odeslaných zpráv v jednotlivých týdnech, v obou případech za posledních deset týdnů. Údaje jsou aktualizovány vždy v pondělí a poskytují přehled již o předcházejícím týdnu.

Na základě takto získaných dat jsou v tabulce níže zaznamenány změny v počtu datových schránek v týdnech od 11.3 do 6.5.2012. K 6.5.2012 bylo v České republice zřízeno celkem 466 987 datových schránek, z údajů je patrné, že každý týden tento počet narůstá v řádech stovek nových datových schránek (MVČR, ©2011).

Týden	Počet nově zřízených DS	Celkový počet DS
11.3.	700	460 103
18.3.	806	460 909
25.3.	678	461 587
1.4.	524	462 111
8.4.	590	462 701
15.4.	351	463 052
22.4.	654	463 706
29.4.	2661	466 367
6.5.	620	466 987

Tabulka 3 – Počet zřízených DS (MVČR, ©2011)

Následující charakteristiky datových schránek jednotlivých subjektů vycházejí především z údajů dostupných na internetových stránkách Portálu veřejné správy, kde je veden seznam držitelů datových schránek dle jednotlivých kategorií. Při porovnání celkového počtu datových schránek na základě údajů ze stránek Datových schránek a Portálu veřejné správy však lze dojít ke zjištění, že výsledné počty se celkově liší o 28 119 datových schránek (k 8.5.2012 zde bylo evidováno 438 868 DS oproti realitě - 466 987 DS). I přesto však jde o nejpřesnější údaje pro získání přehledu o struktuře datových schránek podle subjektů.

Orgánům územní samosprávy bylo zřízeno celkem 6 318 datových schránek, a to v následujících počtech v jednotlivých krajích ČR (seřazeno vzestupně dle počtu DS):

- Hl. m. Praha – 57 DS
- Karlovarský kraj – 133 DS
- Liberecký kraj – 216 DS
- Moravskoslezský kraj – 300 DS
- Zlínský kraj – 306 DS
- Ústecký kraj – 355 DS
- Olomoucký kraj – 400 DS
- Královéhradecký kraj – 449 DS
- Pardubický kraj – 452 DS
- Plzeňský kraj – 502 DS

- Jihočeský kraj – 624 DS
- Jihomoravský kraj – 674 DS
- Vysočina – 705 DS
- Středočeský kraj – 1 145 DS

Orgánům státní správy bylo zřízeno 846 datových schránek.

Ostatním orgánům veřejné moci bylo zřízeno 222 datových schránek.

Soudním exekutorům bylo zřízeno 148 datových schránek.

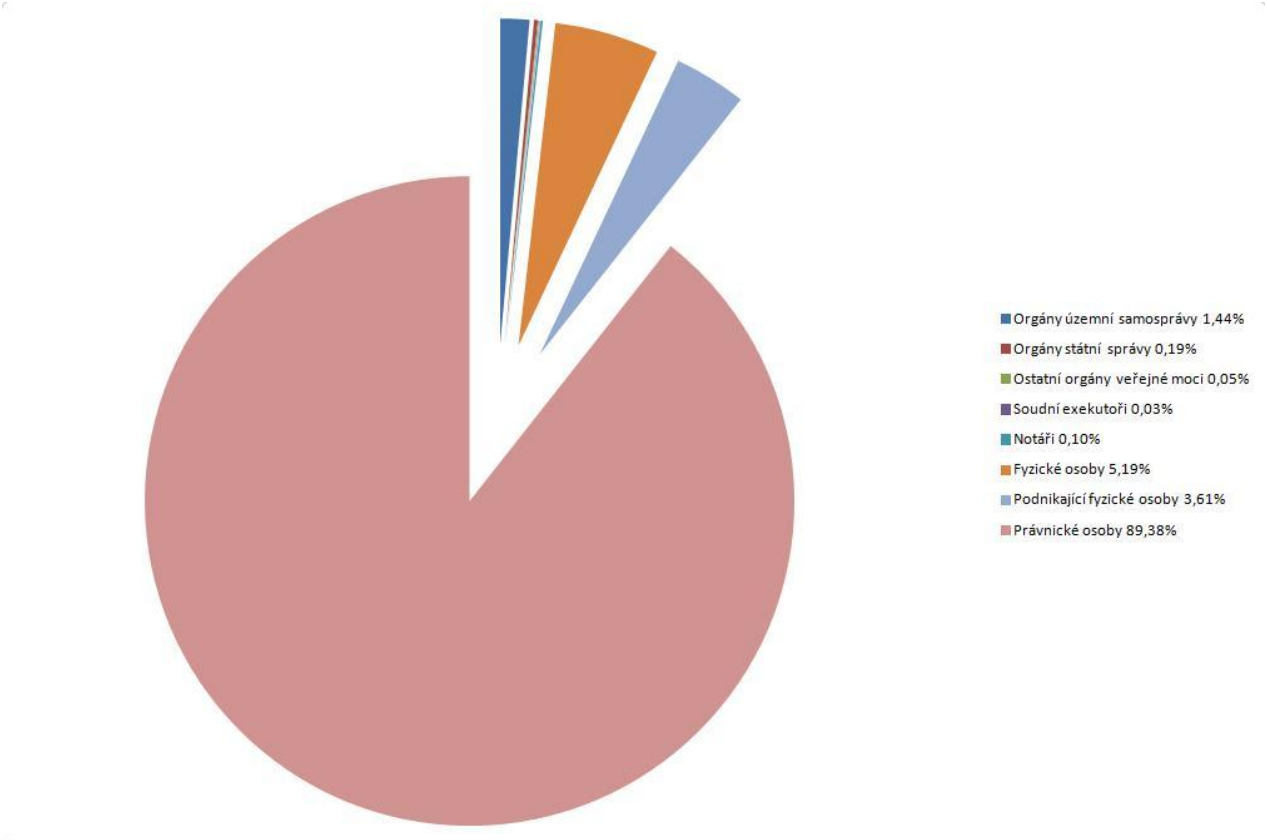
Notářům bylo zřízeno 445 datových schránek.

Fyzickým osobám bylo zřízeno 22 789 datových schránek.

Podnikajícím fyzickým osobám bylo zřízeno 15 851 datových schránek.

Právnickým osobám bylo zřízeno 392 249 datových schránek (MVČR, ©2012).

Pro přehled je k dispozici následující grafické znázornění podílu jednotlivých typů držitelů datových schránek na jejich celkovém počtu:



Obrázek 4 – Poměr držitelů DS (vlastní zpracování)

4.2 Datové zprávy

Do 31.12.2009 bylo možné datové schránky využívat pouze ke komunikaci s orgány veřejné správy (případně k vzájemné komunikaci mezi nimi či ke komunikaci v rámci organizační struktury orgánu), od 1.1.2010 nově byla zavedena možnost datové schránky využít i ke komerční komunikaci pro právnické a fyzické osoby, kdy tímto způsobem mohli držitelé zasílat například faktury. Počínaje červencem 2010 pak bylo možno posílat datové zprávy mezi všemi subjekty, a to bez jakéhokoli omezení co do jejich obsahu.

Grafický přehled o počtu odeslaných datových zpráv je volně dostupný na adrese http://www.datoveschranky.info/, a je tak možno získat tyto informace za posledních deset týdnů, s aktualizací jednou týdně.

Od začátku fungování datových schránek do 6.5.2012 bylo odesláno celkem 80 060 199 datových zpráv. Průměrná úspěšnost doručení přihlášením, tedy kolik ze 100 uživatelů si datovou zprávu přečetlo do deseti dnů od doručení, je aktuálně 97,3%.

Obrázek 5 – Odeslané datové zprávy – týdenní statistiky (MVČR, ©2011)

Aktuální data o odeslaných datových zprávách poskytují pouze informace o jejich celkovém počtu. Zjištění struktury datových zpráv podle subjektů, které je odeslaly, je možné nejaktuálněji získat pouze za rok 2010, a to přímo u provozovatele datových schránek, tedy České pošty, konkrétně tyto údaje zveřejňuje ve výroční zprávě. Ta uvádí, že do prosince 2010 bylo zřízeno celkem 405 942 datových schránek, jejichž prostřednictvím došlo k odeslání 30 441 094 datových zpráv, a to v následujících počtech dle subjektů (Česká pošta, ©2011):

Subjekt	Odeslaných datových zpráv	% podíl
Orgány veřejné moci	28 882 412	94,88
Fyzické osoby	42 392	0,14
Právnické osoby	1 399 306	4,60
Podnikající fyzické osoby	116 984	0,38

Tabulka 4 – Počet odeslaných datových zpráv dle subjektů (Česká pošta, ©2011)

4.3 Statistiky dalších služeb z oblasti datových schránek

Na území České republiky působí celkem tři akreditovaní poskytovatelé certifikačních služeb: První certifikační autorita, a.s., Česká pošta, s.p.(PostSignum) a eIdentity, a.s. Spektrum jimi poskytovaných kvalifikovaných služeb zahrnuje vydávání kvalifikovaných certifikátů, vydávání kvalifikovaných systémových certifikátů a vydávání kvalifikovaných časových razítek.

Nejvyužívanější byla služba PostSignum České pošty, která v roce 2010 vydala celkem 36 710 komerčních a 147 849 kvalifikovaných certifikátů, s 64,9% podílem na trhu, dále vydal v průměru čtyři miliony kvalifikovaných časových razítek měsíčně (Česká pošta, ©2011).

4.4 Spolupráce uživatelů na nových funkcích

V roce 2010 byly datové schránky obohaceny o nové funkce, a to na základě podnětů přímo od uživatelů datových schránek. Informační systém datových schránek tak získal tyto další funkce:

- Filtrování a třídění datových zpráv

- Umožnění vstupu do znepřístupněné datové schránky
- Adresář nejčastěji používaných datových schránek
- Zobrazení doručenky příjemci datové zprávy
- Neomezená platnost hesla (Česká pošta, ©2010)

4.4.1 Filtrování a třídění datových zpráv

Zvláště v případě, kdy je v datové schránce hodně přijatých či odeslaných zpráv, je tato funkce užitečná. Vyhledávání probíhá na základě zadání textu a určení sloupce, kde má být tento text vyhledán, a systém následně uživateli nabídne seznam datových zpráv obsahujících daný text v daném sloupci. Vyhledávat je možné i podle omezení časového období přijetí či odeslání datové zprávy (Česká pošta, ©2010).

4.4.2 Umožnění vstupu do znepřístupněné datové schránky

Před zavedením této funkce bylo nemožné dostat se do datové schránky, která byla znepřístupněna. Po odstranění této překážky však je uživatel schopen datovou schránku využívat pouze v omezeném režimu, může tedy například zobrazit, vytisknout či nechat provést konverzi těch zpráv, které jsou ve schránce , ale nemůže zprávy odesílat či pověřit jinou osobu pro přístup do takové schránky (Česká pošta, ©2010).

4.4.3 Adresář nejčastěji používaných datových schránek

Kromě seznamu identifikátorů („adres“) těch datových schránek, které jsou uživatelem nejvíce využívány, je veden i seznam deseti naposledy použitých, což v závěru vede k úspoře času, komunikuje-li uživatel častěji s některými příjemci (Česká pošta, ©2010).

4.4.4 Zobrazení doručenky příjemci datové zprávy

Teprve po zavedení této funkce se doručenky zobrazují i v seznamu dodaných zpráv, ne jen v seznamu odeslaných zpráv, čímž doručenku může zobrazit nejen odesílatel, ale také adresát (Česká pošta, ©2010).

4.4.5 Neomezená platnost hesla

Neomezenou platnost hesla lze aktivovat změnou nastavení požadavku na opakovanou změnu hesla. Ten je automaticky nastaven v každé datové schránce až do provedení této změny, takže je nutné heslo měnit po devadesáti dnech od předešlé změny. Změnu hesla je doporučeno provádět kvůli zabezpečení datové schránky (Česká pošta, ©2010).

4.5 Využití datových schránek podniky

Jedinou oblastí, kterou v souvislosti s datovými schránkami sleduje Český statistický úřad, je v současnosti využití datových schránek podniků pro zasílání datových zpráv orgánům veřejné správy. Toto využití je rozděleno podle ekonomických činností dle systému CZ-NACE v jednotlivých kategoriích podniků podle počtu zaměstnanců.

V následujících tabulkách jsou jednotlivé podniky dle ekonomické činnosti a počtu zaměstnanců využívající datové schránky ke komunikaci s orgány veřejné správy a jejich procentuální podíl na celkovém počtu v dané velikostní a odvětvové skupině (za rok 2010):

Zpracovatelský průmysl

Ekonomická činnost	Počet zaměstnanců			
	10-49	50-249	250+	Celkem
Potravinářský, nápojový a tabákový průmysl	25,2	69,6	86,9	39,2
Textilní, oděvní, kožedělný a obuvnický průmysl	38,7	71,9	90,5	47,7
Dřevozpracující a papírenský průmysl	36,5	79,9	80,0	44,4
Chemický, farmaceutický, gumárenský a plastový průmysl; Průmysl skla a stavebních hmot	53,3	79,0	77,1	62,3
Výroba kovů, hutních a kovodělných výrobků	46,2	80,6	86,3	56,2
Výroba počítačů, elektronických a optických přístrojů a zařízení	62,1	84,1	96,3	71,9
Výroba elektrických zařízení, výroba strojů a zařízení j. n.	58,3	82,5	83,6	67,4
Automobilový průmysl a výroba ostatních dopravních prostředků	51,9	84,9	83,1	71,5
Výroba nábytku; Ostatní zpracovatelský průmysl; Opravy a instalace strojů a zařízení	45,1	73,9	71,2	52,2
CELKEM	**44,8**	**78,5**	**82,5**	**55,4**

Tabulka 5 – Zpracovatelský průmysl (ČSÚ, ©2012)

Celkově ve zpracovatelském průmyslu datové schránky ke komunikaci s orgány veřejné správy využívá 44,8% podniků s 10-49 zaměstnanci, 78,5% s 50-249 zaměstnanci, 82,5% s 250 a více zaměstnanci, tedy 55,4% všech těchto podniků v České republice (ČSÚ, ©2012).

Výroba a rozvod energie, plynu, vody, tepla a činnosti související s odpady

Ekonomická činnost	Počet zaměstnanců			
	10-49	50-249	250+	Celkem
Stavebnictví	40,4	65,6	75,4	43,8
CELKEM	**59,5**	**65,7**	**75,0**	**62,1**

Tabulka 6 - Výroba a rozvod energie, plynu, vody, tepla a činnosti související s odpady (ČSÚ, ©2012)

Celkově ve výrobě a rozvodu energie, plynu, vody, tepla a v činnostech souvisejících s odpady datové schránky ke komunikaci s orgány veřejné správy využívá 59,5% podniků s 10-49 zaměstnanci, 65,7% s 50-249 zaměstnanci, 75,0% s 250 a více zaměstnanci, tedy 62,1% všech těchto podniků v České republice (ČSÚ, ©2012).

Velkoobchod a maloobchod; Opravy a údržba motorových vozidel

Ekonomická činnost	Počet zaměstnanců			
	10-49	50-249	250+	Celkem
Velkoobchod, maloobchod a opravy motorových vozidel	59,4	80,6	84,4	62,8
Velkoobchod, kromě motorových vozidel	62,0	84,2	89,1	64,6
Maloobchod, kromě motorových vozidel	29,6	39,9	70,4	31,6
CELKEM	**49,5**	**73,5**	**76,8**	**52,3**

Tabulka 7 - Velkoobchod a maloobchod; Opravy a údržba motorových vozidel (ČSÚ, ©2012)

Celkově ve velkoobchodu a maloobchodu a v opravách a údržbě motorových vozidel datové schránky ke komunikaci s orgány veřejné správy využívá 49,5% podniků s 10-49 zaměstnanci, 73,5% s 50-249 zaměstnanci, 76,8% s 250 a více zaměstnanci, tedy 52,3% všech těchto podniků v České republice (ČSÚ, ©2012).

Doprava a skladování

	Počet zaměstnanců			
	10-49	50-249	250+	Celkem
CELKEM	**46,5**	**74,9**	**85,2**	**52,4**

Tabulka 8 – Doprava a skladování (ČSÚ, ©2012)

Celkově v dopravě a skladování datové schránky ke komunikaci s orgány veřejné správy využívá 46,5% podniků s 10-49 zaměstnanci, 74,9% s 50-249 zaměstnanci, 85,2% s 250 a více zaměstnanci, tedy 52,4% všech těchto podniků v České republice (ČSÚ, ©2012).

Ubytování, stravování a pohostinství

Ekonomická činnost	Počet zaměstnanců			
	10-49	50-249	250+	Celkem
Ubytování	40,3	66,7	41,5	43,7
Stravování a pohostinství	29,1	42,9	78,0	30,0
CELKEM	**31,7**	**54,1**	**62,5**	**33,4**

Tabulka 9 – Ubytování, stravování a pohostinství (ČSÚ, ©2012)

Celkově v ubytování, stravování a pohostinství datové schránky ke komunikaci s orgány veřejné správy využívá 31,7% podniků s 10-49 zaměstnanci, 54,1% s 50-249 zaměstnanci, 62,5% s 250 a více zaměstnanci, tedy 33,4% všech těchto podniků v České republice (ČSÚ, ©2012).

Informační a komunikační činnosti

Ekonomická činnost	Počet zaměstnanců			
	10-49	50-249	250+	Celkem
Činnosti v oblasti vydavatelství, filmu, videozáznamů a televizních programů	62,9	85,4	69,5	66,9
Telekomunikační činnosti	65,0	77,3	87,5	68,7
Činnosti v oblasti informačních technologií; Informační činnosti	64,2	72,4	76,6	66,2
CELKEM	**63,9**	**75,6**	**76,5**	**66,6**

Tabulka 10 – Informační a komunikační činnosti (ČSÚ, ©2012)

Celkově v informačních a komunikačních činnostech datové schránky ke komunikaci s orgány veřejné správy využívá 63,9% podniků s 10-49 zaměstnanci, 75,6% s 50-249 zaměstnanci, 76,5% s 250 a více zaměstnanci, tedy 66,6% všech těchto podniků v České republice (ČSÚ, ©2012).

Peněžnictví a pojišťovnictví

	Počet zaměstnanců			
	10-49	50-249	250+	Celkem
CELKEM	**63,4**	**74,8**	**83,6**	**68,9**

Tabulka 11 – Peněžnictví a pojišťovnictví (ČSÚ, ©2012)

Celkově v peněžnictví a pojišťovnictví datové schránky ke komunikaci s orgány veřejné správy využívá 63,4% podniků s 10-49 zaměstnanci, 74,8% s 50-249 zaměstnanci, 83,6% s 250 a více zaměstnanci, tedy 68,9% všech těchto podniků v České republice (ČSÚ, ©2012).

Činnosti v oblasti nemovitostí

	Počet zaměstnanců			
	10-49	50-249	250+	Celkem
CELKEM	**58,8**	**54,2**	**58,0**	**58,5**

Tabulka 12 – Činnosti v oblasti nemovitostí (ČSÚ, ©2012)

Celkově v činnostech v oblasti nemovitostí datové schránky ke komunikaci s orgány veřejné správy využívá 58,8% podniků s 10-49 zaměstnanci, 54,2% s 50-249 zaměstnanci, 58,0% s 250 a více zaměstnanci, tedy 58,5% všech těchto podniků v České republice (ČSÚ, ©2012).

Profesní, vědecké a technické činnosti

	Počet zaměstnanců			
	10-49	50-249	250+	Celkem
CELKEM	**54,2**	**72,7**	**90,5**	**57,0**

Tabulka 13 – Profesní, vědecké a technické činnosti (ČSÚ, ©2012)

Celkově v profesních, vědeckých a technických činnostech datové schránky ke komunikaci s orgány veřejné správy využívá 54,2% podniků s 10-49 zaměstnanci, 72,7% s 50-249 zaměstnanci, 90,5% s 250 a více zaměstnanci, tedy 57,0% všech těchto podniků v České republice (ČSÚ, ©2012).

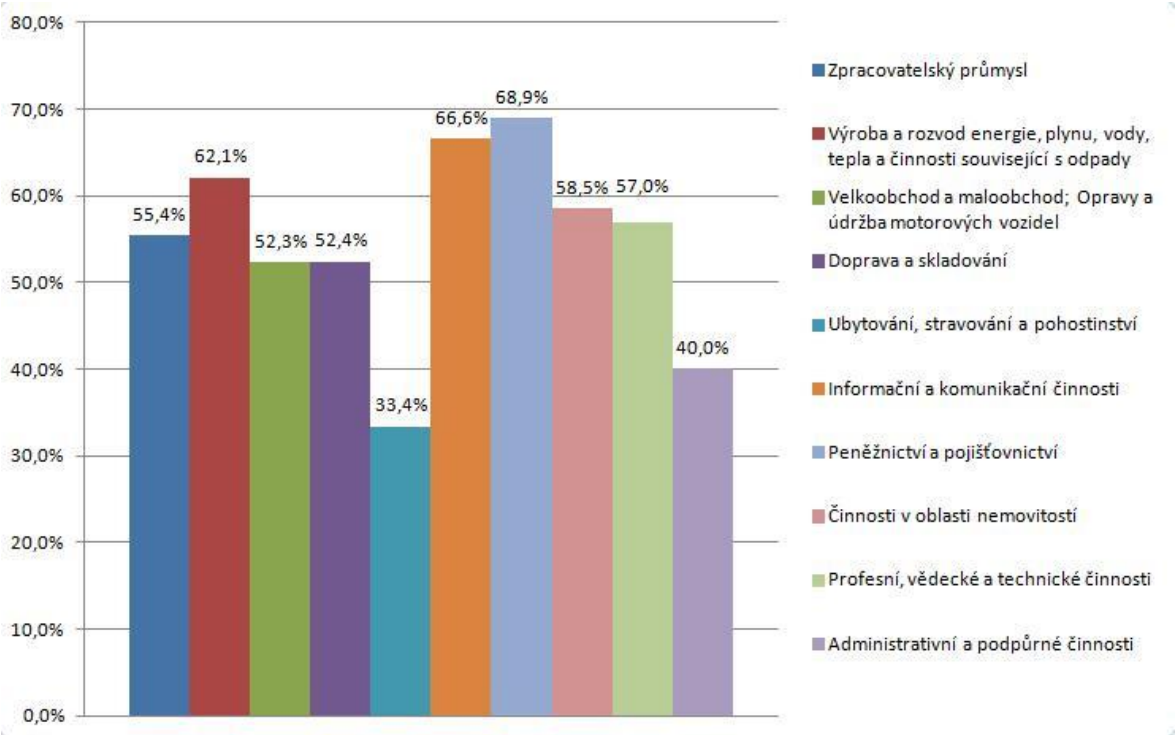
Administrativní a podpůrné činnosti

Ekonomická činnost	Počet zaměstnanců			
	10-49	50-249	250+	Celkem
Činnosti cestovních agentur a kanceláří	44,7	53,8	100,0	46,8
Ostatní administrativní a podpůrné činnosti	30,7	53,6	70,5	39,4
CELKEM	**32,2**	**53,6**	**71,3**	**40,0**

Tabulka 14 – Administrativní a podpůrné činnosti (ČSÚ, ©2012)

Celkově v administrativních a podpůrných činnostech datové schránky ke komunikaci s orgány veřejné správy využívá 32,2% podniků s 10-49 zaměstnanci, 53,6% s 50-249 zaměstnanci, 71,3% s 250 a více zaměstnanci, tedy 40,0% všech těchto podniků v České republice (ČSÚ, ©2012).

V grafu níže je zaznamenáno, kolik procent podniků v daném odvětví využívá datové schránky ke komunikaci s orgány veřejné správy. Z něj je patrné, že největší procento využití datových schránek je s 68,9% u podniků působících v peněžnictví a pojišťovnictví a s 66,6% u podniků v oblasti informačních a komunikačních činností. Naopak nejméně datové schránky využívají podniky z oblasti ubytování, stravování a pohostinství (33,4%) a administrativních a podpůrných činností (40,0%).



Obrázek 6 – Využití DS u podniků dle odvětví (vlastní zpracování)

Celkově datové schránky ke komunikaci s orgány veřejné správy využívá 45,9% podniků s 10-49 zaměstnanci, 72,7% s 50-249 zaměstnanci, 80,1% s 250 a více zaměstnanci, tedy 51,5% všech podniků v České republice (ČSÚ, ©2012).

5 ANALÝZA PROBLÉMŮ SPOJENÝCH S POUŽÍVÁNÍM DATOVÝCH SCHRÁNEK

5.1 Problémy spojené s chováním uživatelů

Systém datových schránek čelí stejně jako jiné servery a počítače s internetovým připojením útokům hackerů. Následné odcizení, změna či zničení doručených dokumentů může mít pak pro dotčeného uživatele závažné důsledky. Pro hackery je mnohem jednodušší zaměřit se přímo na uživatele než zkoušet se nabourat do informačního systému datových schránek. V takovém případě nejsou firmy dostatečně chráněny ani firewally, které používají, ani přihlašovacími údaji či certifikátem (Pavlík, ©2012).

Typ útoku	**Kvalifikace**	**Příležitost**	**Riziko**
Útok na servery datových schránek	vysoká	malá	malé
Útok na šifrovací algoritmy	vysoká	malá	malé
Útoky na klienty			
Fyzické odcizení obálky, hesla, počítače	střední	malá	malé
Bezpečnost prostředí	střední	střední	střední
Bezpečnost aplikací	střední	střední	střední
Chování uživatele u PC	nízká	velká	velké
Sociální útoky	nízká	velká	velké

Tabulka 15 – Typy možných útoků na uživatele datových schránek (Pavlík, ©2012)

5.1.1 Phishing

Phishingové útoky spočívají v získávání přihlašovacích údajů uživatelů datových schránek. Nejčastěji mají podobu e-mailů, u kterých má uživatel dojem, že byly odeslány z ISDS. Po kliknutí na odkaz se uživatel dostane na stránky, které vypadají jako stránky datových schránek, a v okamžiku zadání svých přístupových údajů tyto údaje získají podvodníci (Pavlík, ©2012).

5.1.2 Odcizení hesla z klávesnice

Útoky tohoto typu se provádějí pomocí tzv. keyloggeru, což je software, který zaznamenává zmáčknutí jednotlivých kláves, zejména při zadávání hesel. Tento software se do počítače uživatele může dostat pomocí viru, pokud dochází k instalaci softwaru, který je ilegální, nebo chybou internetového prohlížeče (Pavlík, ©2012).

5.1.3 Krádež relace

Krádež relace je spojena se ztrátou či odcizením notebooku či jiného zařízení, jehož prostřednictvím uskutečňoval uživatel přístup k datové schránce. Takové zařízení má v sobě uložené cookies, což jsou záznamy, jejichž prostřednictvím dochází k připojení k datové schránce. Získáním těchto záznamů pak útočník může získat identitu poškozeného uživatele.

Odposlech síťového provozu mezi uživatelem a serverem je spojen s chybami v internetových prohlížečích a útočník ani nemusí znát heslo, ale převezme snadno obsluhu datové schránky během přihlášení uživatele k webu (Pavlík, ©2012).

5.1.4 DNS poisoning

Služba DNS slouží k převedení doménového jména na IP adresu. IP adresa je tvořena řadou čísel, kterou si uživatelé obtížně zapamatují, a proto IP adresy nahrazují doménovými jmény. Pro vytvoření připojení je IP adresa nutná, a proto DNS doménové jméno na ni převede. Pokud pak uživatel zadá adresu www.datoveschranky.cz, útočník, který získá kontrolu nad serverem poskytovatele internetu, může zachytávat a měnit komunikaci mezi počítačem a DNS, tedy například uživateli nabídne místo pravé stránky pro přihlášení do datové schránky její věrnou kopii, kam on následně zadá své přihlašovací údaje (Pavlík, ©2012).

5.2 Právní rizika

5.2.1 Fikce doručení

Zpráva v datové schránce se automaticky pokládá za doručenou po deseti dnech, a to i tehdy, nedošlo-li uživatelem k vyzvednutí přístupových údajů nebo si schránku sám neaktivoval. Je proto třeba datovou schránku pravidelně kontrolovat její obsah. Fikce do-

ručení může mít pro uživatele závažné důsledky, například začne plynout lhůta pro možné podání odvolání proti úřednímu rozhodnutí (Maisner, ©2012).

5.2.2 Následky zneužití přístupových údajů

Útočník, který získá přístupové údaje k datové schránce, může následně jejím prostřednictvím způsobit uživateli, zejména pak firmám, nemalé škody, které mohou vyústit dokonce v její likvidaci. Dalšími riziky jsou únik důvěrných informací a osobních údajů a využití datové schránky k šíření virů nebo spamů, za což uživateli hrozí sankce, a to až do výše dvaceti milionů korun (Maisner, ©2012).

5.2.3 Archivace datových zpráv po dobu maximálně 90 dnů

Po této době dochází k automatickému smazání datové zprávy z datové schránky uživatele. Následně tak může dojít ke ztrátě dokumentů, které jsou důležité pro právní, daňové či jiné účely (Maisner, ©2012).

5.2.4 Platnost dokumentů vytisknutých z datové schránky

Dokument, který je obsažen v datové zprávě, není platný jen pouhým vytištěním například na domácí tiskárně uživatele bez autorizované konverze do listinné podoby (Maisner, ©2012).

5.2.5 Platnost časového razítka a elektronického podpisu

Platnost těchto složek je časově omezena a u zpráv, které mají pro uživatele dlouhodobější význam, je proto třeba tento problém řešit.

Elektronický podpis je obdobou razítka nebo ručního podpisu na dokumentu v listinné podobě. Jeho platnost je standardně jeden rok. I když při odesílání datové zprávy byl elektronický podpis platný, při následné konverzi již platnost vypršela, a autorizovanou konverzi tak nebylo možné provést. Řešením mělo být kvalifikované časové razítko vstupu. U něj je platnost tři roky. U takových dokumentů, které tak obsahovaly dva elektronické podpisy, nebyla nejdříve autorizovaná konverze možná, nyní ji lze bez problémů provést. Vzhledem k tomu, že tato časová razítka jsou vydávána od roku 2011 a platnosti začnou pozbývat za tři roky, tedy v roce 2014, ukáže se, bude-li konverze možná i potom (Pavlíček, ©2011; Maisner, ©2012).

5.2.6 Doručení poštou namísto prostřednictvím datové schránky

V případě, kdy dokument byl uživateli datové schránky doručen v listinné podobě poštou, ačkoli existují zákonná ustanovení, že měl být doručen do datové schránky, lze spekulovat o tom, lze-li dokument považovat za doručený, a jak se má počítat lhůta, která běží ode dne doručení (Maisner, ©2012).

U správního řádu je třeba rozlišit doručení v rozporu se zákonem a jeho následky. Soudy v případech, kdy dokument byl doručen jiným způsobem, než jaký je stanoven zákonem, zkoumají, došlo-li k tomu, že se adresát s dokumentem seznámil. Jestliže se ukáže, že ano, pak nejsou z nesprávného způsobu doručení vyvozovány žádné negativní účinky. Jestliže tedy adresátovi má být dokument doručen elektronicky, ale byl mu doručen písemně, v případě nepřevzetí či nevyzvednutí není možné se ze strany odesílatele odvolávat na fiktivní doručení po deseti dnech, avšak v situaci, kdy dojde k převzetí zásilky, bude doručení považováno za platné (Burda, ©2011).

5.2.7 Zastupitelnost

Zejména v malých firmách je třeba, aby fungovala kontrola datových schránek statutárním zástupcem, který však musí mít ošetřenou i situaci, kdy má dovolenou nebo je nemocný (Maisner, ©2012).

5.2.8 Spamming a poplatky

Komunikace mezi soukromými uživateli datových schránek funguje od 1.1.2010, od 1.7.2010 si pak kromě elektronických faktur mohou mezi sebou posílat jakékoli zprávy. Odesílatele pak odeslání jedné takové zprávy vyjde na cca 18 Kč, čímž mu může vzniknout velký problém v případě zneužití jeho datové schránky k rozeslání spamu více, nebo dokonce všem, uživatelům datových schránek (Maisner, ©2012).

5.3 Funkční problémy

5.3.1 Datové schránky bez elektronického spisu

Při spuštění projektu datových schránek nebylo jejich fungování spojeno s elektronickým spisem. Ten je veden u insolvenčního řízení (zákon č. 182/2006 Sb., o úpadku a způsobu jeho řešení, ve znění pozdějších předpisů). Od ledna 2012 proběhlo testování

elektronických platebních rozkazů v civilních soudních řízeních, k jejich rozšíření na celé území České republiky by mělo dojít v druhé polovině roku 2012.

U správních a soudních řízení tak stále přetrvává vedení spisů v listinné podobě, což s sebou nese náklady spojené s tiskem jednotlivých dokumentů, jejich převádění do elektronické formy a s tím spojené náklady na pracovníky tyto úkony provádějící. I přes výrazně nižší ceny za doručování datových zpráv prostřednictvím datových schránek je pak výše celkových nákladů srovnatelná s doručováním poštou v listinné podobě.

5.3.2 Datové schránky orgánů veřejné správy

Orgány veřejné správy měly zpočátku pouze jedinou datovou schránku, neexistovala pro ně možnost podání žádosti o zřízení jedné či více dalších datových schránek. Tento stav působil problémy například u katastrálních úřadů (majících jednotlivá katastrální pracoviště), úřadů práce (s detašovanými pracovišti) nebo u obecních úřadů obcí s rozšířenou působností. Tyto orgány musely řešit u svých pracovišť, která se nacházela v různých obcích, jak rozdělovat zásilky. V případě Orgánů sociálněprávní ochrany dětí obecních úřadů obcí s rozšířenou působností nastal problém v okamžiku, kdy bylo do datové schránky obce doručeno předběžné opatření. Tento nedostatek byl však již odstraněn, a to zákonem č. 227/2009 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o základních registrech. Ten je účinný od 24.7.2010, orgány veřejné správy si tedy mohou zažádat o zřízení jedné či více dalších datových schránek (Pavlíček, ©2011; Klang, ©2012).

5.3.3 Datové schránky advokátů

U advokátů a daňových poradců lze datovou schránku zřídit na jejich žádost, a to na základě možného odkladu jejího zřízení ze zákona, který je uveden v zákoně o elektronických úkonech do 31.12.2012. Notáři či exekutoři takovou možnost odkladu nemají. Povinné zřízení datových schránek by přineslo nejen výrazné snížení nákladů, které orgány veřejné správy musejí vynakládat na doručování listinných dokumentů, ale ubylo by také problémů při doručování.

V souvislosti s problematikou datových schránek advokátů je třeba zmínit i fakt, že někteří sice mají datovou schránku zřízenu, avšak pouze jako fyzické osoby. Zejména dříve tak mohlo dojít k doručení datové zprávy určené pro advokáta do datové schránky fyzické osoby. U advokátů, kteří nemají datovou schránku a pracují v advokátní kanceláři (která ji mít musí), pak při doručení jim určené datové zprávy do datové schránky advo-

kátní kanceláře vyvstává rozpor s občanským soudním řádem a dalšími procesními předpisy (Pavlíček, ©2011).

5.4 Ekonomické problémy

Po uplynutí devadesátidenní lhůty ode dne dodání datové zprávy nebo přihlášením datové schránky dojde ke smazání datové zprávy. Pokud je konkrétní dokument pro uživatele důležitý a potřebuje si jej ponechat delší dobu než těchto devadesát dnů, má uživatel možnost nechat provést autorizovanou konverzi, tedy převedení do listinné podoby, nebo využít Datový trezor. Tato služba přesune datovou zprávu, u níž uplynula lhůta devadesáti dnů, do úložiště, kde pak uživatel může datovou zprávu najít a dále s ní pracovat. Službu poskytuje Česká pošta, a to za poplatky uvedené v tabulce níže (Pavlíček, ©2011):

Cena bez DPH za rok	Kapacita datových zpráv
1 200 Kč	100
5 400 Kč	500
48 000 Kč	5 000

Tabulka 16 – Ceník služby Datový trezor (Česká pošta, ©2011)

5.5 Problémy informačních systémů justice

5.5.1 Počítání lhůt

Při počítání lhůt dochází v souvislosti s datovými schránkami k situaci, kdy podle občanského soudního řádu, je-li konec lhůty sobota, neděle či svátek, pak je posledním dnem lhůty následující pracovní den. avšak při doručení do datové schránky dochází k doručení fikcí desátý den ode dne dodání, a to bez ohledu na to, na jaký den konec této lhůty připadá (Pavlíček, ©2011).

Počítání lhůt podle správního řádu se řídí těmito pravidly:

1) začátek lhůty je den, který následuje po dni, kdy vznikla skutečnost určující počátek lhůty
2) u lhůt určených podle týdnů, měsíců či let lhůta končí dnem shodujícím se svým označením se dnem, kdy vznikla skutečnost určující počátek lhůty

Stejně jako u občanského soudního řádu i v tomto případě, je-li konec lhůty sobota, neděle či svátek, pak je posledním dnem lhůty následující pracovní den (ECONNECT, ©2012).

Avšak při doručení do datové schránky dochází k doručení fikcí desátý den ode dne dodání, a to bez ohledu na to, na jaký den konec této lhůty připadá.

5.5.2 Rozlišení oprávněné a pověřené osoby a způsob zaslání datové zprávy

Až do listopadu 2010 nebylo možné zjistit, jestli se do datové schránky přihlásila osoba oprávněná nebo osoba pověřená, protože neexistoval přenos údaje o rozsahu oprávnění. Rozsah oprávnění nebyl v ISDS obsažen, proto ani nemohlo dojít k jeho přenosu do informačního systému justice. Tento problém a také chybějící údaje o způsobu zaslání datové zprávy by pak jistě mohly vést ke zpochybnění platnosti doručení u mnoha dokumentů (Pavlíček, ©2011).

5.5.3 Podání vůči soudům

U podání fyzických, podnikajících fyzických nebo právnických osob bylo až do března 2011 v případě zaslání formou datové zprávy z identifikátoru možno zjistit, zda v elektronickém systému justice došlo k ověření nebo neověření elektronického podpisu. Teprve až koncem roku 2010 došlo k rozšíření skutečnosti, že tento identifikátor neověřuje elektronický podpis osoby, která podání odeslala, ale elektronický podpis Ministerstva spravedlnosti. To mohlo vést k tomu, že řada takových podání nesplňovala podmínky stanovené zákonem, tedy například že podání bylo učiněno osobou s neodpovídajícím rozsahem zákonných oprávnění. Změna identifikátoru proběhla v březnu 2011, i tak je však v případě, že chceme ověřit údaje osoby, která podání provedla, nutné je zjistit v informačním systému justice (Pavlíček, ©2011).

6 NÁVRHY ŘEŠENÍ PROBLÉMŮ SPOJENÝCH S PUŽÍVÁNÍM DATOVÝCH SCHRÁNEK

6.1 Návrhy řešení problémů spojených s chováním uživatelů

Při práci s datovou schránkou a s počítačem obecně je prvním předpokladem pro bezpečnost rozumné chování a uvažování uživatele. Proto například neodpovídá na e-maily, u nichž si není jist původem. Z výše uvedených problémů, které mají vazbu na uživatelské chování, lze správným chováním předejít všem kromě DNS poisoningu.

Pro co nejvyšší možnou bezpečnost existují základní pravidla chování:

1) nestahovat software, který je nelegální a u nějž neznáme původ
2) po dokončení práce s datovou schránkou provést odhlášení, ne jen zavřít okno prohlížeče (Pavlík, ©2012).

6.2 Návrhy řešení právních rizik

6.2.1 Fikce doručení

Pro fyzické a podnikající fyzické osoby, kdy není nikdo jiný s přístupem do jejich datové schránky, je nutné datovou schránku pravidelně kontrolovat, případně si nastavit upozorňování na nové přijaté datové zprávy formou e-mailu, který většinou lidé kontrolují častěji. Nově Česká pošta nabízí i službu SMS upozornění k datové schránce.

Pokud jde o datové schránky organizací, zde je důležité určit zásady, tedy osoby, které mají datovou schránku kontrolovat, intervaly kontroly, ale i následky případně vzniklé škody v souvislosti s jejich selháním kontroly datové schránky (Maisner, ©2012).

6.2.2 Následky zneužití přístupových údajů

Předcházet odcizení přístupových údajů lze tím, že je pečlivě uschováme, vedeme-li si je v podobě poznámky na papíře apod., riziko odcizení přes počítač eliminujeme použitím vhodného zabezpečovacího softwaru. V organizacích je navíc důležité stanovit přísná pravidla v souvislosti s manipulací s přihlašovacími údaji (Maisner, ©2012).

6.2.3 Archivace datových zpráv po dobu maximálně 90 dnů

Předejít tomuto problému lze zvolením vhodného způsobu pro rozšíření informačního systému v oblasti zálohování nebo například službou České pošty Datový trezor.

Služba Datový trezor uvedená jako nástroj pro předejití tomu, aby datová zpráva po uplynutí devadesáti dnů byla automaticky z datové schránky vymazána, je zpoplatněna a zejména pro fyzické osoby, které datové schránky tolik nevyužívají, ale přesto potřebují některé dokumenty uchovat po delší dobu, je jistě tento způsob zbytečně nákladný. Jako alternativní řešení se tak nabízí autorizovaná konverze, kdy je elektronický dokument převeden do listinné podoby za částku 30 Kč za jednu stranu. Méně známou možností pak je uložení dokumentu v datové zprávě do počítače, které uživateli nepřináší žádné nutné poplatky.

Tento problém se pak netýká orgánů veřejné správy. Ty často používají určité elektronické aplikace, kde dochází k ukládání datových zpráv. Navíc disponují vzdáleným přístupem k Czech POINTu, mohou tedy provádět autorizovanou konverzi, a to zcela bez omezení a bez poplatků (Pavlíček, ©2011; Maisner, ©2012).

6.2.4 Platnost dokumentů vytisknutých z datové schránky

Chceme-li dokumenty z datové schránky mít k dispozici v listinné podobě, je pro to, aby měly stejné právní postavení jako originál v elektronické formě, nechat na pracovišti Czech POINT provést autorizovanou konverzi (Maisner, ©2012).

6.2.5 Platnost časového razítka a elektronického podpisu

Platnost elektronické ho podpisu byla částečně vyřešena zavedením časového razítka, není však jasné, jak to bude s možností autorizované konverze po tříleté době, během níž vyprší platnost i časového razítka. Proto lze u opravdu důležitých dokumentů doporučit provedení autorizované konverze do listinné podoby co nejdříve (Pavlíček, ©2011; Maisner, ©2012).

6.2.6 Zastupitelnost

Uživatelům datových schránek systém umožní, aby udělili osobám různá oprávnění pro následnou práci s datovou schránkou. Lze tak v případě potřeby umožnit, aby přijaté datové zprávy četla asistentka v době nepřítomnosti nadřízeného. Oprávnění určuje subjekt, jemuž datová schránka patří a lze je udělit třeba jen na konkrétní úkony, jako je možnost pouze číst přijaté zprávy, pouze datové zprávy odesílat, číst pouze ty, které nebyly určeny do vlastních rukou atd. (Maisner, ©2012).

6.2.7 Spamming a poplatky

Ideálním řešením je kombinace dvou způsobů. Na straně uživatele se jedná o komerční certifikáty České pošty, které však mají tu nevýhodu, že jsou zpoplatněny. Na straně provozovatele, tedy České pošty, by mělo docházet ke sledování systému, a následně by v případě, že existuje podezření, že se jedná o spamming, měla varovat uživatele datové schránky, případně ji i dočasně znepřístupnit (Maisner, ©2012).

6.3 Funkční problémy

6.3.1 Datové schránky advokátů

Řešením problematické situace v oblasti datových schránek advokátů a daňových poradců, tedy zákonem zaručené možnosti odkladu zřízení datové schránky, by bylo vypuštění této výjimky ze zákona. To by vedlo k výrazným úsporám nákladů. Již dnes asi polovina advokátů volí elektronickou formu podání. Druhá polovina stále používá písemnou formu. I tak by však úspora za doručování do datových schránek namísto klasickou poštou byla vyšší než náklady na konverzi listinných dokumentů (Pavlíček, ©2011).

ZÁVĚR

Tato bakalářská práce byla zaměřena na datové schránky a jejich fungování ve veřejné správě. V první části práce se čtenář může seznámit s eGovernmentem, jeho legislativním vymezením, stručnou historií a popisem v rámci Evropské unie a České republiky.

Počínaje druhou kapitolou se práce věnuje informačnímu systému datových schránek, kde je popsána datová schránka, a jsou vysvětleny základní pojmy související s problematikou a čtenáři jsou popsány procesy zřízení, zpřístupnění, znepřístupnění a zrušení datové schránky, kapitola se věnuje jednotlivým subjektům, které vystupují jako uživatelé datových schránek, a jejich specifikům ve vztahu k datovým schránkám.

Poslední kapitola teoretické části je zaměřena na proces zavádění datových schránek v České republice, kde je možno získat o nejpodstatnějších krocích vedoucích k jejich implementaci do systému české elektronické veřejné správy.

V praktické části má čtenář možnost získat přehled o využití datových schránek jednotlivými typy subjektů. Po přečtení kapitoly Analýza problémů spojených s používáním datových schránek získá čtenář přehled o jednotlivých úskalích datových schránek rozřazených do několika skupin podle souvislosti, dále jsou nastíněna řešení některých z uvedených problémů.

SEZNAM POUŽITÉ LITERATURY

[1] ADAPTIC, s. r. o. E-government. *Adaptic* [online]. ©2012 [cit. 2012-04-06]. Dostupné z: http://www.adaptic.cz/znalosti/slovnicek/e-government/

[2] AIP SAFE S.R.O. Datové schránky - dokument management systém je trvalým řešením pro vaše důležité datové zprávy. *Aipsafe* [online]. ©2009 [cit. 2012-04-12]. Dostupné z: http://www.aipsafe.cz/cs/about-us/novinky

[3] AIP SAFE S.R.O. ISDS. *Aipsafe* [online]. ©2009 [cit. 2012-04-12]. Dostupné z: http://www.aipsafe.cz/cs/datove-schranky/pojmy/isds

[4] BUDIŠ, P a HŘEBÍKOVÁ, I. *Datové schránky: fungování, doručování, bezpečnost, návody*. 1. vyd. Olomouc: ANAG, 2010, 287 s. ISBN 978-80-7263-617-4.

[5] CZECHTRADE. Elektronický podpis a jeho využití. *BusinessInfo.cz*: *Oficiální portál pro podnikání a export* [online]. ©2011, [cit. 2012-04-09]. Dostupné z: http://www.businessinfo.cz/cz/clanek/podnikatelske-prostredi/elektronicky-podpis-a-jeho-vyuziti/1001234/2984/

[6] ČESKÁ POŠTA. Poštovní datová zpráva. *Česká pošta* [online]. ©2011 [cit. 2012-04-09]. Dostupné z: http://www.ceskaposta.cz/cz/sluzby/datove-schranky/postovni-datova-zprava-id29096/#1

[7] ČESKÁ POŠTA. Výroční zpráva 2010. *Česká pošta* [online]. ©2011 [cit. 2012-05-08]. Dostupné z: http://www.ceskaposta.cz/assets/o-ceske-poste/profil/ceska-posta_VZ_2010-web.pdf

[8] ČESKÝ STATISTICKÝ ÚŘAD. Informační a komunikační technologie ve veřejné správě 2010. *Český statistický úřad* [online]. ©2012 [cit. 2012-05-10]. Dostupné z: http://www.czso.cz/csu/2011edicniplan.nsf/t/6000370FA6/$File/97031133.pdf

[9] ECONNECT,o.s. Lhůty podle správního řádu. *Econnect - zpravodajství - zprávy* [online]. 2012 [cit. 2012-05-11]. Dostupné z: aa.ecn.cz/img_upload/.../lhuty_SR.rtf

[10] HOLEŠINSKÝ, M. *Analýza problematiky datových schránek a autorizované konverze dokumentů ve státní správě*. Brno, 2009. Dostupné z: http://is.muni.cz/th/208117/fi_b/. Bakalářská práce. Masarykova univerzita, Fakulta informatiky. Vedoucí práce prof. RNDr. Jiří Hřebíček, CSc.

[11] KLANG, M. Papírové spisy u soudů končí. Elektronické jsou rychlejší i levnější. *IDNES.cz* [online]. 2012, [cit. 2012-05-01]. Dostupné z:

http://zpravy.idnes.cz/elektronicke-platebni-rozkazy-pospisil-fdu-/domaci.aspx?c=A120420_091209_ig_zkusenosti_cen

[12] LIDINSKÝ, V. et al. *EGovernment bezpečně*. 1. vyd. Praha: Grada, 2008, 145 s. ISBN 978-80-247-2462-1.

[13] MAGISTRÁT HL. M. PRAHY. K čemu karta slouží. *Opencard*: *Karta pro vaše pohodlí* [online]. ©2010 [cit. 2012-04-09]. Dostupné z: http://opencard.praha.eu/jnp/cz/vyuziti/index.html

[14] MAGISTRÁT HL. M. PRAHY. O kartě. *Opencard*: *Karta pro vaše pohodlí* [online]. ©2010 [cit. 2012-04-09]. Dostupné z: http://opencard.praha.eu/jnp/cz/o_karte/index.html

[15] MAISNER, M. CCB SPOL. S R.O. Datové schránky – na co si dát pozor. *SystemOnLine* [online]. ©2012 [cit. 2012-04-24]. Dostupné z: http://www.systemonline.cz/sprava-dokumentu/datove-schranky-na-co-si-dat-pozor.htm

[16] MASARYKKOVA UNIVERZITA. Historie vývoje eGovernmentu v České republice. In: [online]. Masarykova univerzita, ©2010 [cit. 2012-04-18]. Dostupné z: is.muni.cz/th/143487/fi_m/clanky.doc

[17] MINISTERSTVO VNITRA. Seznam držitelů datových schránek. *Portál veřejné správy* [online]. ©2012 [cit. 2012-05-08]. Dostupné z: http://seznam.gov.cz/ovm/regionList.do

[18] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Autorizovaná konverze. *CzechPOINT* [online]. ©2012 [cit. 2012-04-15]. Dostupné z: http://www.czechpoint.cz/web/index.php?q=node/362

[19] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Czech POINT a E-SHOP České pošty. *Czech POINT* [online]. 2012 [cit. 2012-04-24]. Dostupné z: http://www.czechpoint.cz/web/eshop/

[20] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Státní informační a komunikační politika: e-Česko 2006. *Ministerstvo vnitra České republiky* [online]. ©2004 [cit. 2012-04-07]. Dostupné z: http://aplikace.mvcr.cz/archiv2008/micr/files/275/sikp_def.pdf

[21] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Systém základních registrů. *Ministerstvo vnitra České republiky* [online]. ©2010 [cit. 2012-04-09]. Dostupné z: http://www.mvcr.cz/clanek/egon-symbol-egovernmentu-dokumenty-seznam-zakladnich-registru.aspx?q=Y2hudW09NQ%3d%3d

[22] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Základní registry veřejné správy. *Ministerstvo vnitra České republiky* [online]. ©2010 [cit. 2012-04-07]. Dostupné z: http://www.mvcr.cz/clanek/zakladni-registry-verejne-spravy.aspx

[23] MINISTERSTVO VNITRA ČR. BURDA, Z. Elektronická komunikace se správcem daně (Daně a právo v praxi, 18.7.2011). *Datové schránky* [online]. 2011 [cit. 2012-05-11]. Dostupné z: http://www.datoveschranky.info/cz/tiskovy-servis/napsali-o-nas/elektronicka-komunikace-se-spravcem-dane-dane-a-pravo-v-praxi--18-7-2011-id35164/

[24] MINISTERSTVO VNITRA ČR. Firma - právnická osoba. *Datové schránky* [online]. ©2011 [cit. 2012-04-12]. Dostupné z: http://www.datoveschranky.info/pravnicka-osoba/

[25] MINISTERSTVO VNITRA ČR. Novinky. *Datové schránky* [online]. ©2011 [cit. 2012-05-07]. Dostupné z: http://www.datoveschranky.info/

[26] MINISTERSTVO VNITRA ČR. Občan - fyzická osoba. *Datové schránky* [online]. ©2011 [cit. 2012-04-12]. Dostupné z: http://www.datoveschranky.info/obcan/

[27] MINISTERSTVO VNITRA ČR. Orgán veřejné moci. *Datové schránky* [online]. ©2011 [cit. 2012-04-12]. Dostupné z: http://www.datoveschranky.info/organ-verejne-moci/

[28] MINISTERSTVO VNITRA ČR. Postupy při zřizování datové schránky a žádost. *Datové schránky* [online]. ©2011 [cit. 2012-04-29]. Dostupné z: http://www.datoveschranky.info/assets/metodicke-postupy/zadost_zrizeni_fo.pdf

[29] MINISTERSTVO VNITRA ČR. Postupy při zřizování datové schránky a žádost. *Datové schránky* [online]. ©2011 [cit. 2012-04-29]. Dostupné z: http://www.datoveschranky.info/assets/metodicke-postupy/zadost_zrizeni_pfo.pdf

[30] MINISTERSTVO VNITRA ČR. Postupy při zřizování datové schránky a žádost. *Datové schránky* [online]. ©2011 [cit. 2012-04-29]. Dostupné z: http://www.datoveschranky.info/assets/metodicke-postupy/zadost_zrizeni_po.pdf

[31] MINISTERSTVO VNITRA ČR. Statistiky. *Datové schránky* [online]. ©2011 [cit. 2012-05-08]. Dostupné z: http://www.datoveschranky.info/cz/statistiky-id34635/

[32] MINISTERSTVO VNITRA ČR. Živnostník - podnikající fyzická osoba. *Datové schránky* [online]. ©2011 [cit. 2012-04-12]. Dostupné z: http://www.datoveschranky.info/zivnostnik/

[33] NOVÁK, P. a M. SELICHAROVÁ. ČESKÁ POŠTA. Datové schránky mají na přání uživatelů nové funkcionality. *Česká pošta* [online]. ©2010 [cit. 2012-05-09]. Dostupné z:

http://www.ceskaposta.cz/cz/aktualne/tiskove-zpravy/2010/datove-schranky-maji-na-prani-uzivatelu-nove-funkcionality-id32002/

[34] PAVLÍČEK, T. Problémy fungování datových schránek. In: *COFOLA 2011* [online]. Brno: Masarykova univerzita, 2011 [cit. 2012-05-01]. ISBN 978-80-210-5582-7. Dostupné z: http://www.law.muni.cz/dokumenty/13178

[35] PAVLÍK, R. Běžné chování uživatelů datových schránek znamená bezpečnostní problém. *Egovernment*: *Elektronizace veřejné správy* [online]. ©2012 [cit. 2012-04-23]. Dostupné z: http://www.egovernment.cz/archiv/PDF%204-09/6.pdf

[36] STIEGLER, P. Datové schránky. *Datové schránky* [online]. ©2009 [cit. 2012-04-11]. Dostupné z: http://www.datoveschranky.info/assets/ke-stazeni/datove_schranky-lzofan-stiegler.pdf

[37] ŠTĚDROŇ, B. *Úvod do eGovernmentu v České republice : právní a technický průvodce*. 1. vyd. Praha: Úřad vlády České republiky, 2007, 172 s. ISBN 978-80-87041-25-3.

[38] VANÍČEK, Z. et al. *Právní aspekty eGovernmentu v ČR*. Praha: Linde Praha, 2011, 200 s. ISBN 978-80-7201-855-0.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

a.s.	Akciová společnost
CD	Compact disc
ČR	Česká republika
ČSÚ	Český statistický úřad
DNS	Domain Name System
DPH	Daň z přidané hodnoty
DS	Datová schránky
DVD	Digital Video Disc
EU	Evropská unie
HTML	HyperText Markup Language
IČO	Identifikační číslo organizace
IP	Internet Protocol
IS	Informační systém
ISDS	Informační systém datových schránek
ISOH	Informační systém odpadového hospodářství
ISVS	Informační systémy veřejné správy
kbit/s	Kilobity za sekundu
MB	Megabyte
MVČR	Ministerstvo vnitra České republiky
PDF	Portable Document Format
PDF/A	Portable Document Format/Archive
TXT	Text File
XML	Extensible Markup Language

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: FORMULÁŘ ŽÁDOSTI O ZŘÍZENÍ DATOVÉ SCHRÁNKY FYZICKÉ OSOBY (MVČR, ©2011)

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

datové schránky

I S 2 S a + B f W 6

Žádost o zřízení datové schránky fyzické osoby

podle zákona č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů

Údaje o fyzické osobě

Jméno: | **Příjmení:**

Druhé jméno: | **Rodné příjmení:** | **Datum narození:**

Místo narození

Místo: | **Okres:** | **Stát:** | **Státní občanství:**

Místo trvalého pobytu nebo jiná doručovací adresa (obligatorní údaj dle §37 odst. 2 správního řádu)

Ulice | **Číslo popisné:** | **Číslo orientační:**

Obec: | **PSČ:** | **Stát:**

Nepovinné údaje

pro adresáty, kteří chtějí být vyrozuměni o dodání datové zprávy do datové schránky

Kontaktní e-mail:

Způsoby podání žádosti:

1. Žádost doporučujeme podat osobně na libovolném kontaktním místě veřejné správy Czech POINT. Tento úkon je bezplatný a navíc vám podpis ověří rovnou na místě.
2. Žádost v elektronické podobě opatřete zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb a odešlete na e-podatelnu Ministerstva vnitra (posta@mvcr.cz)
3. Žádost v listinné podobě opatřenou vaším úředně ověřeným podpisem odešlete na kontaktní adresu: Ministerstvo vnitra České republiky, Sekce rozvoje a proj. řízení ICT v oblasti veřejné správy, nám. Hrdinů 1634/3, 140 21 Praha 4.

PŘÍLOHA P II: FORMULÁŘ ŽÁDOSTI O ZŘÍZENÍ DATOVÉ SCHRÁNKY PODNIKAJÍCÍ FYZICKÉ OSOBY (MVČR, ©2011)

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

datové schránky

W h p x a b T L W O

Žádost o zřízení datové schránky podnikající fyzické osoby

podle zákona č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů

Údaje o podnikající fyzické osobě

Jméno:	Příjmení:	
Druhé jméno:	**Rodné příjmení:**	**Datum narození:**

Místo narození

Místo:	Okres:	Stát:	Státní občanství:

Identifikační číslo: (popř. registrační nebo evidenční číslo, nebo jiný obdobný údaj, byl-li přidělen)	Obchodní firma: (Název subjektu)

Adresa místa podnikání

Ulice	Číslo popisné:	Číslo orientační:

Obec:	PSČ:	Stát:	Stát, ve kterém je subjekt registrován:

Nepovinné údaje

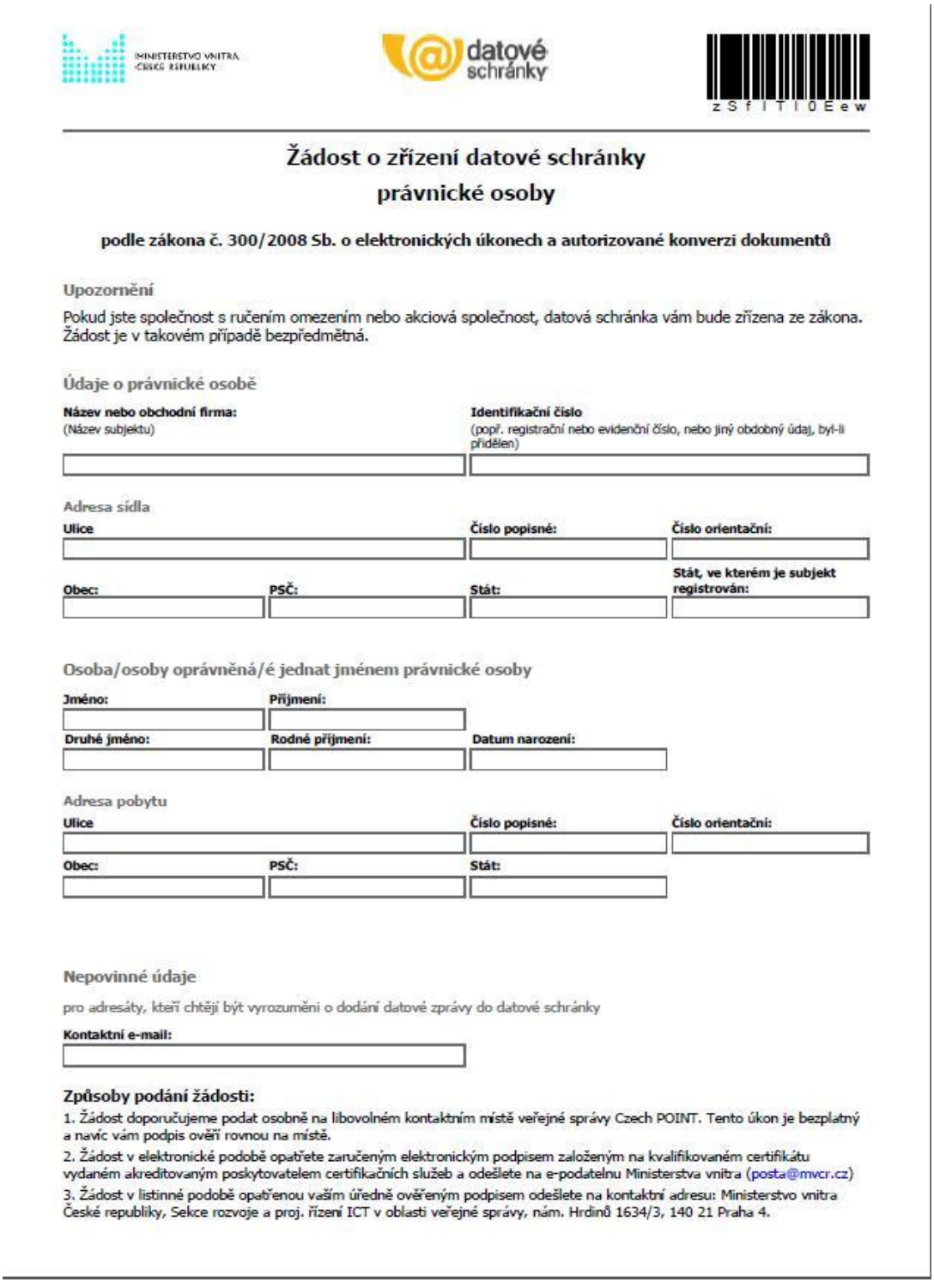
pro adresáty, kteří chtějí být vyrozuměni o dodání datové zprávy do datové schránky

Kontaktní e-mail:

Způsoby podání žádosti:

1. Žádost doporučujeme podat osobně na libovolném kontaktním místě veřejné správy Czech POINT. Tento úkon je bezplatný a navíc vám podpis ověří rovnou na místě.
2. Žádost v elektronické podobě opatřete zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb a odešlete na e-podatelnu Ministerstva vnitra (posta@mvcr.cz)
3. Žádost v listinné podobě opatřenou vaším úředně ověřeným podpisem odešlete na kontaktní adresu: Ministerstvo vnitra České republiky, Sekce rozvoje a proj. řízení ICT v oblasti veřejné správy, nám. Hrdinů 1634/3, 140 21 Praha 4.

PŘÍLOHA P III: FORMULÁŘ ŽÁDOSTI O ZŘÍZENÍ DATOVÉ SCHRÁNKY PRÁVNICKÉ OSOBY (MVČR, ©2011)



MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

datové schránky

zSfITI0Ew

Žádost o zřízení datové schránky právnické osoby

podle zákona č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů

Upozornění

Pokud jste společnost s ručením omezením nebo akciová společnost, datová schránka vám bude zřízena ze zákona. Žádost je v takovém případě bezpředmětná.

Údaje o právnické osobě

Název nebo obchodní firma:
(Název subjektu)

Identifikační číslo
(popř. registrační nebo evidenční číslo, nebo jiný obdobný údaj, byl-li přidělen)

Adresa sídla

Ulice | **Číslo popisné:** | **Číslo orientační:**

Obec: | **PSČ:** | **Stát:** | **Stát, ve kterém je subjekt registrován:**

Osoba/osoby oprávněná/é jednat jménem právnické osoby

Jméno: | **Příjmení:**

Druhé jméno: | **Rodné příjmení:** | **Datum narození:**

Adresa pobytu

Ulice | **Číslo popisné:** | **Číslo orientační:**

Obec: | **PSČ:** | **Stát:**

Nepovinné údaje

pro adresáty, kteří chtějí být vyrozuměni o dodání datové zprávy do datové schránky

Kontaktní e-mail:

Způsoby podání žádosti:

1. Žádost doporučujeme podat osobně na libovolném kontaktním místě veřejné správy Czech POINT. Tento úkon je bezplatný a navíc vám podpis ověří rovnou na místě.
2. Žádost v elektronické podobě opatřete zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb a odešlete na e-podatelnu Ministerstva vnitra (posta@mvcr.cz)
3. Žádost v listinné podobě opatřenou vaším úředně ověřeným podpisem odešlete na kontaktní adresu: Ministerstvo vnitra České republiky, Sekce rozvoje a proj. řízení ICT v oblasti veřejné správy, nám. Hrdinů 1634/3, 140 21 Praha 4.